	<b>NWN Carousel</b> 659 South County Trail Exeter, RI 02822	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NCI001 <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>INFORMATION SECURITY MANUAL</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## TABLE OF CONTENTS

<b>Table of Contents</b> .....	<b>1</b>
<b>Corporate Security Policy:</b> .....	<b>8</b>
<b>Vision, Philosophy and Enforcement</b> .....	<b>8</b>
<b>1.0 Purpose</b> .....	<b>8</b>
<b>2.0 Scope</b> .....	<b>8</b>
<b>3.0 General Security Policies</b> .....	<b>8</b>
<b>4.0 Roles &amp; Responsibilities</b> .....	<b>8</b>
4.1 Security Program .....	8
4.2 NWN Security Committee.....	9
4.3 Owner .....	9
4.4 Custodian .....	9
4.5 User .....	9
4.6 Security Analyst .....	9
4.7 Security Architect.....	9
<b>5.0 Enforcement</b> .....	<b>9</b>
<b>6.0 Review</b> .....	<b>9</b>
<b>Acceptable Use Policy</b> .....	<b>10</b>
<b>1.0 Purpose</b> .....	<b>10</b>
<b>2.0 Scope</b> .....	<b>10</b>
<b>3.0 Goals</b> .....	<b>10</b>
<b>4.0 Policy</b> .....	<b>10</b>
4.1 Ownership of Corporate Technology .....	10
4.2 Security Related Expectations.....	10
4.3 Acceptable Usage.....	10
4.4 Prohibited Activities.....	12
4.5 Monitoring & Privacy Rights .....	14
4.6 Reporting of Security Incident .....	14
4.7 Applicability of Other Policies .....	14
4.8 Enforcement .....	14
<b>5.0 Revision History</b> .....	<b>15</b>
<b>6.0 Approval History</b> .....	<b>15</b>
<b>7.0 Review Cycle</b> .....	<b>15</b>
<b>Asset Management Policy</b> .....	<b>16</b>
<b>1.0 Purpose</b> .....	<b>16</b>
<b>2.0 Scope</b> .....	<b>16</b>
<b>3.0 Goals</b> .....	<b>16</b>
<b>4.0 Policy</b> .....	<b>16</b>
4.1 Ownership of Technology .....	16
4.2 Issued Technology.....	16
4.3 Security Related Expectations.....	16
4.4 Security Banner.....	16
4.5 Asset Tracking .....	16
4.6 Asset Monitoring .....	17
4.7 Asset Audit.....	17
4.8 Minimum Security Baselines.....	17
4.9 Disposal of Information Technology Assets .....	17
4.10 End of Employment .....	17
4.11 Cloud Usage .....	17
4.12 Prohibited Activities.....	18
4.13 Enforcement .....	18
<b>5.0 Revision History</b> .....	<b>18</b>
<b>6.0 Approval History</b> .....	<b>18</b>
<b>7.0 Review Cycle</b> .....	<b>19</b>
<b>Backup Policy</b> .....	<b>20</b>
<b>1.0 Purpose</b> .....	<b>20</b>

<b>2.0</b>	<b>Scope</b> .....	<b>20</b>
<b>3.0</b>	<b>Goals</b> .....	<b>20</b>
<b>4.0</b>	<b>Policy</b> .....	<b>20</b>
4.1	Responsibilities .....	20
4.2	Identification of Critical Data .....	20
4.3	Data to be Backed Up .....	20
4.4	Data that does not meet the Criteria for Backup .....	20
4.5	Access to Backups .....	21
4.6	Backup Scheme .....	21
4.7	Backup Schedule .....	21
4.8	Backup Location .....	21
4.9	Backup Retention .....	21
4.10	Restoration Procedures & Documentation .....	21
4.11	Restoration Testing .....	21
4.12	Request for Backup Restoration .....	21
4.13	Backup to Cloud .....	21
4.14	Audit of Backup Files .....	21
4.15	Applicability of Other Policies .....	22
4.16	Enforcement .....	22
<b>5.0</b>	<b>Approval History</b> .....	<b>22</b>
<b>6.0</b>	<b>Review Cycle</b> .....	<b>22</b>
<b>Classification Policy</b> .....		<b>23</b>
<b>1.0</b>	<b>Purpose</b> .....	<b>23</b>
<b>2.0</b>	<b>Scope</b> .....	<b>23</b>
<b>3.0</b>	<b>Goals</b> .....	<b>23</b>
<b>4.0</b>	<b>Policy</b> .....	<b>23</b>
4.1	Data Classification .....	23
4.2	Data Storage .....	23
4.3	Data Transmission .....	23
4.4	Data Destruction .....	24
4.5	Applicability of Other Policies .....	24
4.6	Enforcement .....	24
<b>5.0</b>	<b>Revision History</b> .....	<b>24</b>
<b>6.0</b>	<b>Approval History</b> .....	<b>25</b>
<b>7.0</b>	<b>Review Cycle</b> .....	<b>25</b>
<b>Confidential Data Policy</b> .....		<b>26</b>
<b>1.0</b>	<b>Purpose</b> .....	<b>26</b>
<b>2.0</b>	<b>Scope</b> .....	<b>26</b>
<b>3.0</b>	<b>Goals</b> .....	<b>26</b>
<b>4.0</b>	<b>Policy</b> .....	<b>26</b>
4.1	Treatment of Confidential Data .....	26
4.2	Use of Confidential Data .....	26
4.3	Security Controls for Confidential Data .....	27
4.4	Examples of Confidential Data .....	27
4.5	Clear Desk Policy .....	27
4.6	Applicability of Other Policies .....	28
4.7	Enforcement .....	28
<b>5.0</b>	<b>Revision History</b> .....	<b>28</b>
<b>6.0</b>	<b>Approval History</b> .....	<b>28</b>
<b>7.0</b>	<b>Review Cycle</b> .....	<b>28</b>
<b>Electronic Communications Policy</b> .....		<b>29</b>
<b>1.0</b>	<b>Purpose</b> .....	<b>29</b>
<b>2.0</b>	<b>Scope</b> .....	<b>29</b>
<b>3.0</b>	<b>Goals</b> .....	<b>29</b>
<b>4.0</b>	<b>Policy</b> .....	<b>29</b>
4.1	Proper Use of Company Electronic Communication Systems .....	29
4.2	External and/or Personal Email Accounts .....	31
4.3	Confidential Data and Electronic Communications .....	31
4.4	Company Administration of Electronic Communications .....	32
4.5	Prohibited Actions .....	33
4.6	Data Leakage .....	33
4.7	Sending Large Emails .....	33
4.8	Monitoring & Privacy Rights .....	33
4.9	Applicability of Other Policies .....	34
4.10	Enforcement .....	34
<b>5.0</b>	<b>Revision History</b> .....	<b>34</b>


6.0	<i>Approval History</i> .....	34
7.0	<i>Review Cycle</i> .....	34
<b>Employee Administration Policy</b> .....		<b>35</b>
1.0	<i>Purpose</i> .....	35
2.0	<i>Scope</i> .....	35
3.0	<i>Goal</i> .....	35
4.0	<i>Policy</i> .....	35
4.1	Employee Management Requirements .....	35
4.2	Employee Screening .....	35
4.3	Onboarding .....	35
4.4	Employee Transfer .....	36
4.5	Termination .....	36
4.6	Monitoring & Privacy Rights .....	36
4.7	Applicability of Other Policies .....	36
5.0	<i>Revision History</i> .....	36
6.0	<i>Approval History</i> .....	36
7.0	<i>Review Cycle</i> .....	37
<b>Encryption Policy</b> .....		<b>38</b>
1.0	<i>Purpose</i> .....	38
2.0	<i>Scope</i> .....	38
3.0	<i>Goals</i> .....	38
4.0	<i>Policy</i> .....	38
4.1	Applicability of Encryption .....	38
4.2	Encryption Key Management .....	38
4.3	Acceptable Encryption Algorithms .....	38
4.4	Legal Use .....	39
5.0	<i>Revision History</i> .....	39
6.0	<i>Approval History</i> .....	39
7.0	<i>Review Cycle</i> .....	39
<b>External Supplier Management Policy</b> .....		<b>40</b>
1.0	<i>Purpose</i> .....	40
2.0	<i>Scope</i> .....	40
3.0	<i>Goals</i> .....	40
4.0	<i>Policy</i> .....	40
4.1	Evaluating a Provider .....	40
4.2	Contracts .....	40
4.3	Security Controls .....	40
4.4	Applicability of Other Policies .....	41
4.5	Security Compliance .....	41
4.6	Enforcement .....	41
5.0	<i>Revision History</i> .....	41
6.0	<i>Approval History</i> .....	41
7.0	<i>Review Cycle</i> .....	42
<b>Guest Wireless Network Policy</b> .....		<b>43</b>
1.0	<i>Purpose</i> .....	43
2.0	<i>Scope</i> .....	43
3.0	<i>Goals</i> .....	43
4.0	<i>Policy</i> .....	43
4.1	Guest Access .....	43
4.2	Restrictions on Guest Access .....	43
4.3	Monitoring & Privacy Rights .....	43
4.4	Guest Access Infrastructure Requirements .....	43
4.5	Audits .....	43
4.6	Applicability of Other Policies .....	43
4.7	Enforcement .....	44
5.0	<i>Revision History</i> .....	44
6.0	<i>Approval History</i> .....	44
7.0	<i>Review Cycle</i> .....	44
<b>Incident Response Policy</b> .....		<b>45</b>
1.0	<i>Purpose</i> .....	45
2.0	<i>Scope</i> .....	45
3.0	<i>Goals</i> .....	45
4.0	<i>Policy</i> .....	45
4.1	Types of Incidents .....	45
4.2	Incident Response Plan .....	45
4.3	Reporting of Security Incident .....	45
4.4	Preparation .....	45

4.5	Confidentiality .....	45
4.6	Electronic Incidents.....	46
4.7	Physical Incidents.....	46
4.8	Notification .....	46
4.9	Event Logging.....	47
4.10	Managing Risk.....	47
4.11	Breach of Personally Identifiable Information (PII).....	47
4.12	Applicability of Other Policies .....	47
4.13	Enforcement .....	47
<b>5.0</b>	<b>Revision History .....</b>	<b>47</b>
<b>6.0</b>	<b>Approval History .....</b>	<b>48</b>
<b>7.0</b>	<b>Review Cycle.....</b>	<b>48</b>
<b>Mobile Device Policy .....</b>		<b>49</b>
<b>1.0</b>	<b>Purpose .....</b>	<b>49</b>
<b>2.0</b>	<b>Scope.....</b>	<b>49</b>
<b>3.0</b>	<b>Goals .....</b>	<b>49</b>
<b>4.0</b>	<b>Policy.....</b>	<b>49</b>
4.1	General Guidelines.....	49
4.2	Mobile Device Management.....	49
4.3	Data Security.....	49
4.4	Device Protection.....	50
4.5	Connecting to Unsecured Networks .....	50
4.6	Personal Mobile Devices.....	50
4.7	Replacement Device Request .....	50
4.8	Mobile Device Monitoring .....	50
4.9	Mobile Devices and Motor Vehicles.....	50
4.10	End of Employment .....	50
4.11	Applicability of Other Policies .....	50
4.12	Enforcement .....	50
<b>5.0</b>	<b>Revision History .....</b>	<b>51</b>
<b>6.0</b>	<b>Approval History .....</b>	<b>51</b>
<b>7.0</b>	<b>Review Cycle.....</b>	<b>51</b>
<b>Network Access &amp; Authentication Policy .....</b>		<b>52</b>
<b>1.0</b>	<b>Purpose .....</b>	<b>52</b>
<b>2.0</b>	<b>Scope.....</b>	<b>52</b>
<b>3.0</b>	<b>Goals .....</b>	<b>52</b>
<b>4.0</b>	<b>Policy.....</b>	<b>52</b>
4.1	Account Setup.....	52
4.2	Account Use.....	52
4.3	Multifactor Authentication .....	52
4.4	Account Termination .....	53
4.5	Account Suspension.....	53
4.6	Name Policy .....	53
4.7	Authentication .....	53
4.8	Use of Passwords .....	53
4.9	Remote Network Access.....	53
4.10	Screensaver Passwords.....	53
4.11	Minimum Configuration for Access.....	54
4.12	Encryption.....	54
4.13	Failed Logons .....	54
4.14	Non-Business Hours.....	54
4.15	Administrator Accounts .....	54
4.16	Applicability of Other Policies .....	54
4.17	Enforcement .....	54
<b>5.0</b>	<b>Revision History .....</b>	<b>54</b>
<b>6.0</b>	<b>Approval History .....</b>	<b>54</b>
<b>7.0</b>	<b>Review Cycle.....</b>	<b>55</b>
<b>Network Security Policy .....</b>		<b>56</b>
<b>1.0</b>	<b>Purpose .....</b>	<b>56</b>
<b>2.0</b>	<b>Scope.....</b>	<b>56</b>
<b>3.0</b>	<b>Goals .....</b>	<b>56</b>
<b>4.0</b>	<b>Policy.....</b>	<b>56</b>
4.1	Network Device Passwords.....	56
4.2	Logging.....	56
4.3	Firewalls.....	57
4.4	Networking Hardware.....	57

4.5	Network Servers .....	58
4.6	Collaborative Devices.....	58
4.7	Intrusion Detection/Intrusion Prevention.....	58
4.8	Security Testing.....	58
4.9	Audit Security.....	59
4.10	Disposal of Information Technology Assets .....	59
4.11	Network Compartmentalization .....	59
4.12	Network Documentation .....	60
4.13	Antivirus/Anti-Malware .....	60
4.14	Software Use Policy .....	60
4.15	Maintenance Windows and Scheduled Downtime .....	60
4.16	Change Management.....	60
4.17	Suspected Security Incidents .....	60
4.18	Redundancy .....	60
4.19	Manufacturer Support Contracts .....	61
4.20	Security Policy Compliance .....	61
4.21	Applicability of Other Policies .....	62
4.22	Enforcement .....	62
<b>5.0</b>	<b>Revision History .....</b>	<b>62</b>
<b>6.0</b>	<b>Approval History .....</b>	<b>62</b>
<b>7.0</b>	<b>Review Cycle.....</b>	<b>62</b>
<b>Password Policy .....</b>		<b>63</b>
<b>1.0</b>	<b>Purpose .....</b>	<b>63</b>
<b>2.0</b>	<b>Scope.....</b>	<b>63</b>
<b>3.0</b>	<b>Goals .....</b>	<b>63</b>
<b>4.0</b>	<b>Policy.....</b>	<b>63</b>
4.1	Requirements .....	63
4.2	Confidentiality .....	63
4.3	Change Frequency .....	64
4.4	Multifactor Authentication .....	64
4.5	Incident Reporting .....	64
4.6	Administrator Accounts .....	64
4.7	Failed Logons .....	64
4.8	Applicability of Other Policies .....	64
4.9	Enforcement .....	64
<b>5.0</b>	<b>Revision History .....</b>	<b>64</b>
<b>6.0</b>	<b>Approval History .....</b>	<b>65</b>
<b>7.0</b>	<b>Review Cycle.....</b>	<b>65</b>
<b>Patch Management Policy.....</b>		<b>66</b>
<b>1.0</b>	<b>Purpose .....</b>	<b>66</b>
<b>2.0</b>	<b>Scope.....</b>	<b>66</b>
<b>3.0</b>	<b>Goals .....</b>	<b>66</b>
<b>4.0</b>	<b>Patch Management .....</b>	<b>66</b>
4.1	Patch Identification.....	66
4.2	Patch Testing.....	66
4.3	Patch Deployment .....	66
4.4	Vulnerability Scanning .....	66
4.5	System End of Life/End of Support .....	67
4.6	Integrity Verification Tools.....	67
4.7	Applicability of Other Policies .....	67
4.8	Enforcement .....	67
<b>5.0</b>	<b>Revision History .....</b>	<b>67</b>
<b>6.0</b>	<b>Approval History .....</b>	<b>67</b>
<b>7.0</b>	<b>Review Cycle.....</b>	<b>67</b>
<b>Physical Security Policy .....</b>		<b>68</b>
<b>1.0</b>	<b>Purpose .....</b>	<b>68</b>
<b>2.0</b>	<b>Scope.....</b>	<b>68</b>
<b>3.0</b>	<b>Goals .....</b>	<b>68</b>
<b>4.0</b>	<b>Policy.....</b>	<b>68</b>
4.1	Choosing a Site.....	68
4.2	Security Zones.....	68
4.3	Access Controls .....	69
4.4	Physical Data Security .....	69
4.5	Physical System Security .....	69
4.6	Electrical Considerations.....	70
4.7	Fire Prevention .....	70

4.8	Entry Security .....	70
4.9	Removal of Equipment from Data Centers .....	71
4.10	Applicability of Other Policies .....	71
4.11	Enforcement .....	71
<b>5.0</b>	<b>Revision History .....</b>	<b>71</b>
<b>6.0</b>	<b>Approval History .....</b>	<b>72</b>
<b>7.0</b>	<b>Review Cycle .....</b>	<b>72</b>
<b>Privacy Policy .....</b>		<b>73</b>
<b>1.0</b>	<b>Purpose .....</b>	<b>73</b>
<b>2.0</b>	<b>Scope .....</b>	<b>73</b>
<b>3.0</b>	<b>Goals .....</b>	<b>73</b>
<b>4.0</b>	<b>Policy .....</b>	<b>73</b>
4.1	Information Security Standards .....	73
4.2	Information Security Awareness Program .....	74
4.3	Enforcement .....	74
<b>5.0</b>	<b>Revision History .....</b>	<b>75</b>
<b>6.0</b>	<b>Approval History .....</b>	<b>75</b>
<b>7.0</b>	<b>Review Cycle .....</b>	<b>75</b>
<b>Remote Access Policy .....</b>		<b>76</b>
<b>1.0</b>	<b>Purpose .....</b>	<b>76</b>
<b>2.0</b>	<b>Scope .....</b>	<b>76</b>
<b>3.0</b>	<b>Goals .....</b>	<b>76</b>
<b>4.0</b>	<b>Policy .....</b>	<b>76</b>
4.1	Prohibited Actions .....	76
4.2	Non-Company Provided Machines .....	76
4.3	Client Software .....	76
4.4	Network Access .....	76
4.5	Idle Connections .....	76
4.6	Applicability of Other Policies .....	76
4.7	Enforcement .....	77
<b>5.0</b>	<b>Revision History .....</b>	<b>77</b>
<b>6.0</b>	<b>Approval History .....</b>	<b>77</b>
<b>7.0</b>	<b>Review Cycle .....</b>	<b>77</b>
<b>Retention Policy .....</b>		<b>78</b>
<b>1.0</b>	<b>Purpose .....</b>	<b>78</b>
<b>2.0</b>	<b>Scope .....</b>	<b>78</b>
<b>3.0</b>	<b>Goals .....</b>	<b>78</b>
<b>4.0</b>	<b>Policy .....</b>	<b>78</b>
4.1	Reasons for Data Retention .....	78
4.2	Data Duplication .....	78
4.3	Retention Requirements .....	78
4.4	Retention of Encrypted Data .....	79
4.5	Legal Hold .....	79
4.6	Data Destruction .....	79
4.7	Applicability of Other Policies .....	79
4.8	Enforcement .....	79
<b>5.0</b>	<b>Revision History .....</b>	<b>79</b>
<b>6.0</b>	<b>Approval History .....</b>	<b>79</b>
<b>7.0</b>	<b>Review Cycle .....</b>	<b>80</b>
<b>Third Party Connection Policy .....</b>		<b>81</b>
<b>1.0</b>	<b>Purpose .....</b>	<b>81</b>
<b>2.0</b>	<b>Scope .....</b>	<b>81</b>
<b>3.0</b>	<b>Goals .....</b>	<b>81</b>
<b>4.0</b>	<b>Policy .....</b>	<b>81</b>
4.1	Use of Third Party Connections .....	81
4.2	Security of Third Party Access .....	81
4.3	Restricting Third Party Access .....	81
4.4	Offshore Connections .....	81
4.5	Auditing of Connections .....	82
4.6	Applicability of Other Policies .....	82
4.7	Enforcement .....	82
<b>5.0</b>	<b>Revision History .....</b>	<b>82</b>
<b>6.0</b>	<b>Approval History .....</b>	<b>82</b>
<b>7.0</b>	<b>Review Cycle .....</b>	<b>83</b>
<b>Virtual Private Network (VPN) Policy .....</b>		<b>84</b>
<b>1.0</b>	<b>Purpose .....</b>	<b>84</b>
<b>2.0</b>	<b>Scope .....</b>	<b>84</b>

<b>3.0</b>	<b>Goals</b>	<b>84</b>
<b>4.0</b>	<b>Policy</b>	<b>84</b>
4.1	Encryption	84
4.2	Authentication	84
4.3	Implementation	84
4.4	Management	84
4.5	Logging and Monitoring	84
4.6	Encryption Keys	84
4.7	Applicability of Other Policies	84
4.8	Enforcement	85
<b>5.0</b>	<b>Revision History</b>	<b>85</b>
<b>6.0</b>	<b>Approval History</b>	<b>85</b>
<b>7.0</b>	<b>Review Cycle</b>	<b>85</b>
<b>Wireless Network Policy</b>		<b>86</b>
<b>1.0</b>	<b>Purpose</b>	<b>86</b>
<b>2.0</b>	<b>Scope</b>	<b>86</b>
<b>3.0</b>	<b>Goals</b>	<b>86</b>
<b>4.0</b>	<b>Policy</b>	<b>86</b>
4.1	Physical Guidelines	86
4.2	Configuration and Installation	86
4.3	Inactivity	87
4.4	Guest Access	87
4.5	Monitoring & Privacy Rights	87
4.6	Applicability of Other Policies	87
4.7	Enforcement	87
<b>5.0</b>	<b>Revision History</b>	<b>87</b>
<b>6.0</b>	<b>Approval History</b>	<b>87</b>
<b>7.0</b>	<b>Review Cycle</b>	<b>88</b>
<b>Glossary</b>		<b>89</b>
<b>Index</b>		<b>93</b>
<b>Change Management Log</b>		<b>94</b>

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NCI001-A <b>Version:</b> 1.2
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>CORPORATE SECURITY POLICY:          VISION, PHILOSOPHY AND ENFORCEMENT</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

The foundation of an effective information security program is built on strong information security policies that are in balance with business operations. Information security policies define a concise set of behaviors that provide a secure and enabling environment in which NWN Carousel may use and manage its information resources. NWN Carousel Information Security Policy represents the combined efforts of the Information Services (IS), Human Resources (HR) and Legal departments, as well as the user communities. These policies have been presented to and approved by executive management.

NWN Carousel requires an Information Security Policy to accomplish its business objectives in a secure and timely manner. Instituting an Information Security Policy demonstrates the commitment that NWN Carousel has to safeguarding customer and corporate information assets. That commitment must extend from each individual involved in business operations. Providing written, organization-wide policies is the most efficient, fair manner of information protection. Some advantages of the Information Security Policy Program are:

- Demonstrates management's commitment to the protection of information assets.
- Builds effectiveness, efficiency and adaptability into information security.
- Informs all NWN Carousel employees of corporate philosophy and requirements.
- Deters potential illicit activity by demonstrating management's commitment to security.
- Provides a mechanism for demonstrating "due diligence" against potential legal and financial liabilities.

The overall authority of the Information Security Program is with the Executive Vice President of Customer Success (EVP CS). Management of the Information Security Program is delegated to the members of the Security Committee. The overall success of the program is dependent upon adherence to the policy and enforcement by Management, IS, HR, the Legal Department and the user community.

Due to the rapid pace of technological and operational growth, policies can become outdated and lose their effectiveness. NWN Carousel will respond to this problem by soliciting feedback from users and custodians and reviewing policies annually. This is a minimum requirement. Some policies may be updated more frequently due to momentous technological advances.

The Executive Vice President of Customer Success, or their designee, will ensure updates and new policies are published and distributed periodically. When necessary, policy updates will be distributed immediately.

## 2.0 Scope

The NWN Carousel Corporate Security Policy applies to all employees, interns, contractors, vendors and anyone using NWN information assets. Information assets are defined as any information system (hardware or software), data, networks and components owned or leased by NWN Carousel or designated representatives. Policies are the organizational mechanism used to manage the confidentiality, integrity and availability of information assets.

## 3.0 General Security Policies

The NWN General Security Policy describes the foundation of the Corporate Information Security Program. Information Security Policies are the principles that direct managerial decision-making and facilitate secure business operations. A concise set of security policies enables NWN to manage the security of information assets and maintain accountability. These policies provide the security framework upon which all subsequent security efforts will be based. They define the appropriate and authorized behavior for personnel approved to use NWN information assets.

## 4.0 Roles & Responsibilities

### 4.1 Security Program

The Director of Security Risk & Compliance is responsible for setting strategic direction, creating policies and monitoring compliance of the Information Security Program. All decisions not already covered by policies detailed herein will be escalated to individual for final decision.



## **4.2 NWN Security Committee**

The NWN Security Committee is responsible for overseeing the development, implementation and maintenance of the NWN's information security program, including assigning specific responsibility for its implementation and reviewing reports from management. The current members of the NWN Security Committee are the Executive Vice President of Customer Success, Vice President of Technology Operations, General Counsel, Director of Human Resources, Senior Vice President of Customer Experience, Director of Security Risk and Compliance, Director of Information Technology and Director of Cloud Operations. The Security Architects in conjunction with the CSOIT teams are responsible for the implementation and execution of the Security Policy.

## **4.3 Owner**

The designated individual responsible for the business use of information and information systems or networks. The owner assigns value to the specified information set, authorizes access to that information, specifies protective measures to the custodian and users of the information and determines retention and privacy of the information.

## **4.4 Custodian**

The individual tasked to process, store and protect the information assets, as specified by the owner. This responsibility includes following physical, technical and procedural guidelines and safeguards established to protect information.

## **4.5 User**

The authorized individual who accesses, adds, modifies, or deletes information as originally prescribed by the owner. Specific user responsibilities will be defined throughout the NWN Security Policy.

## **4.6 Security Analyst**

The Security Analyst role is held by the customer Success Technology Operations Center. The Customer Success Technology Operations Center monitors and triage all security alerts generated by the security tooling used to monitor and protect the environment. Should there be any security incidents that require further triage, investigation or engineering, those incidents will be escalated to the CSOIT team or the CSET teams depending on the incident details.

## **4.7 Security Architect**

The Security Architect role is held by three positions within NWN. Each role has responsibility around separate pieces of the environment. The Cloud Operations Team Lead position holds the security architect responsibility for the Hosted Collaboration and Contact Center environments. The Senior Solution Engineer of the CSOIT team holds the security architect responsibility for NWN Carousel systems and the Principal Consultant of Security holds the security architect roles for new offerings and emerging technologies


## **5.0 Enforcement**

Compliance with NWN Carousel Information Security Policy is mandatory. Exceptions to these policies must be approved in writing by the EVP CS or their designee.

Violators of any policy are subject to disciplinary actions including termination and/or civil and criminal legal action.

## **6.0 Review**

This policy will be reviewed and agreed to by all employees upon hire and on an annual basis thereafter. Additionally, the NWN Carousel Security Committee will revalidate this Information Security Manual, which includes the employee Acceptable Use Policy, annually in conjunction with the HCS System Security Plan.

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NCI001-B <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>ACCEPTABLE USE POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

This Acceptable Use Policy details how corporate Information Technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is additionally asked to use common sense when using company resources. Any questions on what constitutes the Acceptable Usage of company resources should be directed to CSOIT.

## 2.0 Scope

This policy applies to all employees, contractors, guests or other individual who uses any and all of the corporate Information Technology resources including, but not limited to, production & lab computer systems, email, networks, and the Corporate Network.

## 3.0 Goals

Since inappropriate use of corporate systems exposes both NWN Carousel and its customers to risk, it is important to specify exactly what is permitted and what is prohibited. The goal of this policy is to detail the acceptable use of corporate Information Technology resources for the protection of NWN Carousel systems and networks and our customer’s information.

## 4.0 Policy

### 4.1 Ownership of Corporate Technology

The information technology resources provided and maintained by NWN Carousel are intended for business related purposes including administrative functions and for the support of our customers. In the case of “issued technology,” NWN Carousel retains ownership of said technology and the data contained within. The business will monitor and regulate the usage of all issued technology to ensure the integrity of its data and compliance with industry standards. CSOIT may access any and all information technology resources at any time in accordance with company Information Security Policies.

### 4.2 Security Related Expectations

Information Security Standards have been implemented in order to protect the company, its Information Technology resources and data. Users are expected to adhere to all NWN Carousel security standards including the following:

- All technology must have time-out enabled and be password protected.
- Passwords must follow the guidelines stated in the Password Policy.
- Mobile devices that contain company data must be kept secure against possible theft.
- Corporate Technology Resources may not be used for any illegal activities.

### 4.3 Acceptable Usage

#### 4.3.a Issued Technology

NWN Carousel issued technology is intended to aid employees in the performance of their job duties. Employees who are issued technology by NWN Carousel are expected to take care of the equipment and to be prepared to return the equipment upon request. This includes, but is not limited to, computers, mobile devices, storage media, VPN phones, etc. For any issues or questions pertaining to Corporate Technology, please contact CSOIT for assistance.

#### 4.3.b Network Access

NWN Carousel adheres to the “principles of least privilege.” This means that users will only be given access to the information and programs that are required in their job functions. Users should make all reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access.

#### 4.3.c Email

The corporate email system is provided to employees for business communications only. Personal usage of company email systems is prohibited. The following contains examples of unacceptable use of the email system. For further information, please refer to the Email Policy.

- The following is never permitted: spamming, harassment, communicating threat solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.
- Users are prohibited from forging email header information or attempting to impersonate another person (This is not intended to prohibit instances of delegation).
- Email is an unsecure method of communication, and thus information that is considered confidential or proprietary to NWN Carousel may not be sent via email, regardless of the recipient, without proper encryption.
- It is company policy not to open email attachments from unknown senders, or when such attachments are unexpected.
- Email systems were not designed to transfer large files and as such, emails should not contain attachments of excessive file size.

#### **4.3.d Instant Message**

Instant messaging provides a valuable form of communication in both a personal and professional setting. It is with this in mind that the business provides an internal instant messaging service for selected employees and allows for personal instant messaging during lunch and on breaks for all employees. Users are reminded that instant messaging is subject to monitoring by CSOIT. It should also be noted that Instant Messaging is an unsecure medium and that users are expected follow all applicable Information Security Policies, especially in regards to the disclosure of confidential data. It is with this in mind that NWN Carousel also prohibits the transfer of files to federated customers through Instant Message as these communications even though they are technically encrypted.

#### **4.3.e Internet**

NWN Carousel recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of company computer systems to access the Internet is permitted during lunch, breaks, and before/after business hours, as long as such usage follows pertinent policies and guidelines and does not have a detrimental effect on NWN Carousel or on the user's job performance. Users are reminded that Internet usage conducted on the corporate network is monitored and that excessive use or abuse of this privilege can result in disciplinary action, up to and including termination.

NWN Carousel manages access to certain websites that fall into specific categories with network security appliances to ensure compliance with security standards. Individual managers have the right to restrict Internet access further for their specific department.

Employees should accept that the internet is an unsecured medium and as such, he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. Employees use the Internet at their own risk and NWN Carousel is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

#### **4.3.f Social Media**

NWN Carousel acknowledges both the benefit and widespread use of social networking as a tool for communication. It is with this in mind that the business allows the use of social networking sites during lunch, breaks, and before/after working hours. Users are reminded that Internet usage conducted on the corporate network is monitored and that excessive use or abuse of this privilege can result in disciplinary action. NWN Carousel expects that employees will conduct themselves in a professional manner when blogging or on social media sites when representing the company. Users also assume all risks associated with blogging and/or social networking.

#### **4.3.g Consumer Mobile Devices**

The use of personal mobile devices is allowed at NWN Carousel. However, in order to safe guard company information and to comply with security standards, employees who connect to the corporate network with their personal mobile device must agree and comply with the following:

- Must allow CSOIT administrative access to their device so that it is compliant with NWN Carousel Standards.
- All devices that connect to the corporate network must be password protected.
- Users are responsible for keeping device secure from theft (i.e. do not leave device in plain sight in an unlocked car)
- NWN Carousel monitors all connections to the corporate data by personal devices.
- NWN Carousel reserves the right to physically inspect, remote audit and wipe all data from devices that have connected to the corporate network.
- User must immediately report loss or theft to CSOIT.
- Personal mobile devices that contain business data are not allowed to sync with unauthorized

- devices (i.e. personal/home computers, other personal devices, etc.)
- Any device that contains business information is not to be shared with other individuals.
- CSOIT currently supports iPhone's operating system, iOS, and a limited number of models that run an Android Operating System. CSOIT cannot guarantee the compatibility or accessibility of unsupported models with the corporate network.
- Tampering with any security controls put in place by CSOIT is prohibited.
- The act of connecting a personal mobile device to NWN Carousel Network requires the employee to adhere to all applicable Security Policies and guidelines.
- All data stored on personal devices remains the property of NWN Carousel and may be controlled, monitored, or removed at any time including during a security incident or in case of termination.

#### **4.3.h Personal Storage Media**

Personal storage devices represent a serious threat to data security and are expressly prohibited on NWN Carousel network unless they are issued or approved by NWN Carousel.

#### **4.3.i User Network Drive**

The User/Shared Network Drives are accessible by employees to aid in the retention of business documents when storage on computers is limited. Due to restrictions on size, the following applies to all user/shared drives on the network:

- The User/Shared drives are intended for business documents only.
- Non-work related pictures, music, videos, web pages, and any other personal files are prohibited.
- There is no increase in size for User Drives
- The business does not backup information stored on User Drives
- All User/Shared Drives can be cleaned at CSOIT's discretion

#### **4.3.j Remote Desktop Access**

Use of remote desktop software and/or services is allowable as long as it is approved and provided by NWN Carousel. Remote access to the network must conform to NWN Carousel Remote Access Policy.

#### **4.3.k Confidential Data**

Confidential data must not be:

- Shared or disclosed in any manner to non-employees of NWN Carousel
- Must not be posted on the Internet or any publicly accessible systems
- Will not be transferred in any unsecure manner. Please refer to the Confidential Data Policy for further information.

#### **4.3.l Streaming Media**

In an attempt to limit bandwidth usage, streaming media is permitted for business use only. The use of streaming media sites will be monitored and regulated by CSOIT.

#### **4.3.m Software**

Installation of non-company-supplied or approved programs is prohibited. Numerous security threats can masquerade as innocuous software – viruses, malware, spyware, and trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance. CSOIT reserves the right to remove any non-approved applications installed on Corporate owned devices.

### **4.4 Prohibited Activities**

#### **4.4.a Non-Company Owned Equipment**

Non-company provided equipment is expressly prohibited on NWN Carousel network. This includes all privately owned computers, flash storage, and mobile devices that have not been authorized for access by CSOIT. Exceptions to this policy:

- Exceptions may be granted to the devices of Contractors who have undergone a thorough security analysis to ensure the devices meet or exceed NWN Carousel standards.
- C-Level executives may exclude an employee this policy to allow a personal device with valid reasoning of request
- If an exception is granted, the following stipulations apply:
  - The personal device is subject to the entirety of the NWN Carousel Security Policy
  - The device will be configured in full accordance with NWN Carousel Corporate Security Standards.

- NWN Carousel must obtain the personal device and ensure compliance of the security standard which includes but is not limited to:
- NWN Carousel IT to have Full Administration access of the device
- Installation of NWN Carousel standard issue security and monitoring software
- The personal device is subject to all data monitoring described in this the Information Security Policy
- Offboarding will include a full wipe of the device in accordance with DoD 5220.22-M to ensure the secure erasure of the data contained on the drive
- Device shall not be used to connect to customer or managed services networks

#### **4.4.b Bandwidth Consumption**

Excessive use of company bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed using approved mechanisms. Please contact CSOIT prior to commencing large or bulk file/data transfers.

#### **4.4.c Unacceptable Use of Network**

The following actions shall constitute unacceptable use of the corporate network. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate network and/or systems to:

- Engage in activity that is illegal under local, state, federal, or international law.
- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to NWN Carousel and its customers.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Engage in activities that cause an invasion of privacy.
- Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
- Make fraudulent offers for products or services.
- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function.
- Install or distribute unlicensed or "pirated" software.
- Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

#### **4.4.d Tampering With Technology**

All technology issued to Carousel employees has been configured by CSOIT to ensure the security of information residing on the device and the integrity of the Corporate Network. It is with this in mind that employees are expressly forbidden from altering issued technology in such a way that it may compromise the security of their device or the corporate network. The following are examples of prohibited modifications to issued technology:

- Disabling/removing anti-virus
- Altering firewall settings
- Upgrading/modifying any physical component without express consent from CSOIT

#### **4.4.e Illegal Activities**

No company-owned or company-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning
- Unauthorized Network Hacking
- Unauthorized Packet Sniffing or Spoofing
- Unauthorized Denial of Service
- Unauthorized Wireless Hacking
- Acts of Terrorism
- Identity Theft
- Spying
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system

NWN Carousel will take all necessary steps to report and prosecute any violations of this policy.

#### **4.4.f Copyright Infringement**

NWN Carousel computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner:

- Copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's;
- Posting or plagiarizing copyrighted material; and
- Downloading copyrighted files which employee has not already legally procured. This list is not meant to be exhaustive, copyright law applies to a wide variety of media and applies to much more than is listed above.

#### **4.4.g P2P File Sharing**

Peer-to-Peer (P2P) networking is not allowed on the corporate network under any circumstance.

#### **4.4.h Circumvention of Security**

Using company-owned or company-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any physical or electronic actions to bypass or circumvent security is expressly prohibited.

#### **4.4.i Neglect of Technology**

In circumstances where an employee has demonstrated continual abuse or neglect with NWN Carousel technology, CSOIT reserves the right to initiate administrative action. This action could include, but is not limited to, issuance of low-cost technology alternative, refusal to issue technology, notifying the employee's manager for remediation, notifying Human Resources for documentation within the employee's record, or termination. In the case of an employee being denied technology, the employee may expense the cost of usage but not that of a new device. All complaints of technology neglect will be reviewed by CSOIT on a case-by-case basis.

### **4.5 Monitoring & Privacy Rights**

Users should have no expectation of privacy when using the corporate electronic communication systems, corporate provided devices, or other approved devices by NWN Carousel. This includes, but is not limited to, geographical data, transmission and/or storage of files, data, and all personal & business emails. CSOIT is continuously monitoring the corporate network, and by extent, all devices connected to it. This monitoring is done to ensure the integrity of the network and to ensure compliance with established security policies. CSOIT may access any and all information technology resources at any time in accordance with company Information Security Policies.

### **4.6 Reporting of Security Incident**

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and/or contact CSOIT or Human Resource as detailed in the corporate Incident Response Policy. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Suspected virus/malware/Trojan infection.
- Loss or theft of any device that contains company information.
- Loss or theft of ID badge or keycard.
- Any attempt by any person to obtain a user's password over the telephone or by email.
- Any other suspicious event that may impact NWN Carousel information security.

Users must treat a suspected security incident as confidential information, and report the incident only to his or her supervisor. Users must not withhold information relating to a security incident or interfere with an investigation.

### **4.7 Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

### **4.8 Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and

including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

## 5.0 Revision History


Name	Date	Brief Description of Changes	Version
James Aiello	8/26/11	Reformatted Acceptable Use Policy	Version 1.1
James Aiello	11/4/11	Revised Acceptable Use Policy per CIIMT Audit	Version 2.0
James Aiello	9/29/14	Revised Acceptable Use Policy per CIIMT Audit	Version 2.1
James Aiello	4/14/15	Edited Acceptable Use Policy per CIIMT Audit.	Version 2.2
James Aiello	8/20/16	Edited Acceptable Use Policy per CIIMT Audit.	Version 2.3
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.4
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.5
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

## 6.0 Approval History

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methe	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

## 7.0 Review Cycle

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	9/29/14	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NCI001-C <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>ASSET MANAGEMENT POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

The purpose of the IT Asset Management Policy is to maintain accurate records of NWN’s assets. This document establishes procedures to ensure compliance with government regulations, legal industry standards and to ensure accurate reporting of physical assets.

## 2.0 Scope

This policy applies to all hardware and software assets issued and/or owned by NWN Carousel that will transmit, process, or store NWN Carousel or Customer data.

## 3.0 Goals

To ensure the tracking and management of all technology assets across the various teams and locations of NWN Carousel.

## 4.0 Policy

### 4.1 Ownership of Technology

The technology resources provided and maintained by NWN Carousel are intended for business related purposes including administrative functions and for the support of our customers. In the case of “issued technology,” NWN Carousel retains ownership of said technology and the data contained within. The business will monitor and regulate the usage of all technology to ensure the integrity of its data and compliance with industry standards. CSOIT may access any and all information technology resources at any time in accordance with company Information Security Policies.

### 4.2 Issued Technology

NWN Carousel issued technology is intended to aid employees in the performance of their job duties. Employees who are issued technology by NWN Carousel are expected to take care of the equipment and to be prepared to return the equipment upon request. This includes, but is not limited to, computers, mobile devices, storage media, VPN phones, etc. For any issues or questions pertaining to Corporate Technology, please contact CSOIT for assistance.

### 4.3 Security Related Expectations

Information Security Standards have been implemented in order to protect the company, its Information Technology resources and data. Users are expected to adhere to all NWN Carousel security standards including the following:

- All technology must have time-out enabled and be password protected.
- Passwords must follow the guidelines stated in the Password Policy.
- Mobile devices that contain company data must be kept secure against possible theft.
- Corporate Technology Resources may not be used for any illegal activities.

### 4.4 Security Banner

All corporate computing systems will display appropriate legal warnings for improper access and use of corporate systems. End user devices, Servers, Infrastructure Devices (firewalls, switches, routers) and Remote Access devices will be configured with the following banner:

*THIS COMPUTER SYSTEM INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES ARE PROVIDED FOR LEGITIMATE BUSINESS PURPOSES ONLY. UNAUTHORIZED ACCESS, USE, OR MODIFICATION OF THIS SYSTEM IS STRICTLY PROHIBITED. USE OF THIS COMPUTER SYSTEM CONSTITUTES EXPRESS CONSENT TO MONITORING AND RECORDING OF ANY ACTIONS TAKEN WHILE USING THIS SYSTEM. EVIDENCE COLLECTED DURING MONITORING MAY BE USED IN LEGAL PROCEEDINGS OR DISCIPLINARY ACTIONS. UNAUTHORIZED USE MAY BE PUNISHABLE BY TERMINATION OR CRIMINAL OR CIVIL LITIGATION.*

### 4.5 Asset Tracking

All end user workstations, mobile devices, portable storage devices, Access Points, Remote Access Points’ (RAPs), switches and firewalls must have an Asset Tag or be tracked by a unique identifier (ie. Serial number)



and be entered into the Asset Tracking Database prior to deployment. Information Assets will be tracked within the database and assigned an “owner” who will be the primary stakeholder for that application. Each profile must include the model number, serial numbers, software version and licensing details in order to meet business and industry standards. The database will be kept current with the asset, if returned to CSOIT it will be assigned to “Stock” until it is deployed to another user.

#### **4.6 Asset Monitoring**

CSOIT actively monitors all activity on Corporate owned devices, including mobile devices. This can take the form of network monitoring, logging of all activity including non-work related. All mobile devices will be tracked using geo-location software, for tracking the geographical location of these devices, in the event they become lost or are stolen. Employees should not have expectation of privacy while using company provided equipment. NWN monitors the geographic location of all remote access attempts, and may prohibit access based on certain locations.

#### **4.7 Asset Audit**

Periodic audits will be performed for all technology tracked in the Asset Tracking Database. Identified abnormalities will be investigated and verified by CSOIT. All Carousel employees are required to assist CSOIT with this audit by validating their assigned equipment when requested.

#### **4.8 Minimum Security Baselines**

Where able, all hardware will be configured with the document Minimum Security Baselines (MSB) established by the Internal Infrastructure Team. Said MSB’s will be created for all technology, where applicable, including networking hardware, end user workstations, and mobile devices.

#### **4.9 Disposal of Information Technology Assets**

CSOIT assets, such as network servers, routers, or workstations often contain sensitive data about NWN Carousel and/or our customers information. When assets are decommissioned, the following guidelines must be followed:

- Any asset tags or stickers that identify NWN Carousel must be removed before disposal.
- Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.
- Data storage hardware must be wiped in accordance with DoD 5220.22-M to ensure the secure erasure of the data contained on the drive. Alternatively, the physical destruction of the device’s data storage mechanism (such as its hard drive or solid state memory) is required. If physical destruction is not possible, the CSOIT Management must be notified.

#### **4.10 End of Employment**

When a user’s employment comes to an end at NWN Carousel, they are required to return all issued devices to CSOIT or Human Resources within 10 business days. If equipment is not returned in a timely manner, NWN Carousel may report the equipment as stolen to local police and initiate legal action to remedy the situation.

#### **4.11 Cloud Usage**

Cloud usage by employees, whether using NWN’s property and systems or personal computer systems, are also subject to the terms and restrictions set forth in this Policy. This cloud usage policy is meant to ensure that cloud services are NOT used without the CSOIT Team’s /CS EVP’s knowledge. It is imperative that employees NOT open cloud services accounts or enter into cloud service contracts for the storage, manipulation or exchange of company-related communications or company-owned data without the CSOIT Team’s /CS EVP’s input. This is necessary to protect the integrity and confidentiality of NWN data and the security of the network.

NWN remains committed to enabling employees to do their jobs as efficiently as possible through the use of technology. The following guidelines are intended to establish a process whereby NWN employees can use cloud services without jeopardizing company data and computing resources:

- Use of cloud computing services for work purposes must be formally authorized by the CSOIT Team/CS EVP. The CSOIT Team/CS EVP will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor.
- For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by Counsel, the CSOIT Team/CS EVP.
- The use of such services must comply with NWN’s existing Acceptable Use Policy/Computer Usage Policy/Internet Usage Policy.
- Employees must not share log-in credentials with co-workers. The CSOIT Team will keep a confidential document containing account information for business continuity purposes.
- The use of such services must comply with all laws and regulations governing the handling of personally

- identifiable information, corporate financial data or any other data owned or collected by NWN.
- The CSOIT Team /CS EVP decides what data may or may not be stored in the cloud.
- Personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data.

## **4.12 Prohibited Activities**

### **4.12.a Tampering with Technology**

All technology issued to NWN Carousel employees has been configured by CSOIT to ensure the security of information residing on the device and the integrity of the Corporate Network. It is with this in mind that employees are expressly forbidden from altering issued technology in such a way that it may compromise the security of their device or the corporate network. The following are examples of prohibited modifications to issued technology:

- Disabling anti-virus
- Altering firewall settings
- Upgrading/modifying any physical component without express consent from CSOIT

### **4.12.b Circumvention of Security**

Using company-owned or company-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any physical or electronic actions to bypass or circumvent security is expressly prohibited.

### **4.12.c Neglect of Technology**

In circumstances where an employee has demonstrated continual abuse or neglect with NWN Carousel technology, CSOIT reserves the right to initiate administrative action. This action could include, but is not limited to, issuance of low-cost technology alternative, refusal to issue technology, notifying the employee's manager for remediation, notifying Human Resources for documentation within the employee's record. In the case of an employee being denied technology, the employee may expense the cost of usage but not that of a new device. All complaints of technology neglect will be reviewed by CSOIT on a case-by-case basis.

## **4.13 Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

## **5.0 Revision History**

<b>Name</b>	<b>Date</b>	<b>Brief Description of Changes</b>	<b>Version</b>
Eads, Butch	2/12/16	Reformatted Acceptable Use Policy	Version 1.0
Aiello, James	01/20/17	Revised Acceptable Use Policy per CIIMT Audit	Version 1.1
Aiello, James	03/03/18	Revised Acceptable Use Policy per CIIMT Audit	Version 1.2
Aiello, James	02/17/19	Edited Acceptable Use Policy per CIIMT Audit.	Version 1.3
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1


## **6.0 Approval History**

<b>Approved By</b>	<b>Title</b>	<b>Version Approved</b>	<b>Date Approved</b>
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23

NWN Carousel Security Committee			5/19/23
---------------------------------	--	--	---------

**7.0 Review Cycle**

<b>Review Cycle</b>	<b>Scheduled Review Date</b>	<b>Reviewer</b>	<b>Status-Action Needed</b>
Annual	06/01/13	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NCI001-D <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>BACKUP POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

A backup policy is similar to an insurance policy, it provides the last line of defense against data loss and is sometimes the only way to recover from a hardware failure, data corruption, or a security incident. The Backup Policy is related closely to a disaster recovery policy, but since it protects against events that are relatively likely to occur, in practice it will be used more frequently than a contingency planning document.

## 2.0 Scope

This policy applies to all data stored on corporate systems. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

## 3.0 Goals

The goal of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

## 4.0 Policy

### 4.1 Responsibilities

#### 4.1.a CSOIT

Below are responsibilities of CSOIT regarding backups:

- Identify systems and applications that need to be backed up.
- Implement backups in accordance with defined standards.
- Administration of backup files and recovery requests
- Perform regular tests of the backups to ensure data files can be recovered
- Audit backups in accordance with the Retention Policy

#### 4.1.b NWN Carousel's Employees

Employees are reminded that NWN Carousel does not perform scheduled backups on individual workstations. Users are encouraged to upload any critical documents to operational team portals and NWN Carousel approved cloud services to perform a backup of their machine on a regular basis. For instructions on performing a system backup, please contact CSOIT for assistance.

### 4.2 Identification of Critical Data

NWN Carousel must identify what data is most critical to its organization. This is done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data must be identified so that it can be given the highest priority during the backup process.

### 4.3 Data to be Backed Up

A backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up will include:

- All data determined to be critical to company operation and/or employee job function.
- All information stored on the corporate file server(s) and email server(s). It is the user's responsibility to ensure any data of importance is moved to the file server.
- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, network appliances, remote access servers, etc.

### 4.4 Data that does not meet the Criteria for Backup

NWN Carousel does not wish to simply adopt a "save everything" mentality. That is not practical or cost-effective, and would place an excessive and unnecessary burden on the business and the CSOIT team to manage the constantly growing amount of data. Data that meets any of the following criteria will be excluded from consideration for corporate backup and will not be included in any centralized backup solutions.

- Data that is older than 24 months.
- Data that has not been accessed within the past 24 months.

- End user personal files or information such as the following.
  - Personal photos
  - Personal music collections
  - Personal information

#### **4.5 Access to Backups**

Due to the critical nature of backups, access will be restricted to approved members of CSOIT.

#### **4.6 Backup Scheme**

The backup scheme is critical to successful data recovery. CSOIT has determined that the scheme will be implemented based on the type, classification, confidentiality and BCDR requirements to allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator.

#### **4.7 Backup Schedule**

The backup schedule is the second critical piece to a successful data recovery plan. A backup can be programmed to run hourly, nightly, weekly. The schedule of backups will be dependent on the classification of the program being backed up and the backup scheme being utilized.

#### **4.8 Backup Location**

Geographic separation from the backups must be maintained, to some degree, to protect from fire, flood, or other regional or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data, which must meet NWN Carousel uptime requirements.

#### **4.9 Backup Retention**

When determining the time required for backup retention, NWN Carousel must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data. NWN Carousel has determined that the following will meet all requirements (note that the backup retention policy must confirm to NWN Carousel data retention policy and any industry regulations, if applicable):

- Daily backups are overwritten the next day.
- Full backups must be saved for three months.
- Incremental backups must be saved for two weeks.
- Weekly backups are kept for 6 weeks.
- Monthly backups must be saved for 6 months.

#### **4.10 Restoration Procedures & Documentation**

The data restoration procedures must be tested and documented. Documentation should include the responsible parties for the restore, what is to be restored, how it is performed, and under what circumstances it is to be performed. It is extremely important that the procedures are clear and concise such that they are not A) misinterpreted by readers other than the backup administrator, and B) confusing during a time of crisis.

#### **4.11 Restoration Testing**

It is important to periodically test the restore procedures to eliminate potential problems. Backup restores must be tested when any change is made that may affect the backup system, which must include a manual restore on key systems.

#### **4.12 Request for Backup Restoration**

Requests for a restoration of a backup must be submitted to CSOIT in the form of a ticket. Due to the nature of a restoration, it must be thoroughly researched for impact to the business by CSOIT prior to approval.

#### **4.13 Backup to Cloud**

##### **4.13.a Employee Backup to 3<sup>rd</sup> Party Cloud**

NWN Carousel does not allow employees to backup or upload business documents to non-approved cloud services. This includes, but is not limited to, iCloud, Google Play, Amazon Cloud, Carbonite, etc.

##### **4.13.b Corporate Backup to 3<sup>rd</sup> Party Cloud**

CSOIT reserves the right to also backup business data to a cloud based service. This service must be thoroughly vetted to ensure they meet NWN Carousel Information Security Standards and then approved my management prior to the upload of any data.

#### **4.14 Audit of Backup Files**

Backups will be audited on a quarterly basis in accordance with the Retention Policy and industry standards.

#### 4.15 Applicability of Other Policies

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

#### 4.16 Enforcement

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.


James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1
Name	Date	Brief Description of Changes	Version
James Aiello	08/01/11	Reformatted Backup Policy	Version 1.1
James Aiello	10/31/11	Reformatted Backup Policy	Version 1.2
James Aiello	11/9/12	Edited per Information Security Audit	Version 2.0
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.1
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.2
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

#### 5.0 Approval History

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

#### 6.0 Review Cycle

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	11/9/12	CIIMT	Completed
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> 659 South County Trail Exeter, RI 02822	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NCI001-E <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>CLASSIFICATION POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

Information assets are assets to NWN Carousel just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to company operations and the confidentiality of its contents. Once this has been determined, NWN Carousel can take steps to ensure that data is treated appropriately.

## 2.0 Scope

The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location. Also covered by the policy are hardcopies of company data, such as printouts, faxes, notes, etc.

## 3.0 Goals

The goal of this Classification Policy is to detail a method for classifying data and to specify how to handle this data once it has been classified.

## 4.0 Policy

### 4.1 Data Classification

Data residing on corporate systems must be continually evaluated and classified into the following categories:

- **Personal:** includes user's personal data, emails, documents, etc. This policy excludes personal information, so no further guidelines apply.
- **Public:** includes already-released marketing material, commonly known information, etc. There are no requirements for public information.
- **Operational:** includes data for basic business operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.
- **Critical:** any information deemed critical to business operations (often this data is operational or confidential as well). It is extremely important to identify critical data for security and backup purposes.
- **Confidential:** any information deemed proprietary to the business. See the Confidential Data Policy for more detailed information about how to handle confidential data.

### 4.2 Data Storage

The following guidelines apply to storage of the different types of company data.

#### 4.2.a Personal

There are no requirements for personal information.

#### 4.2.b Public

There are no requirements for public information.

#### 4.2.c Operational

Operational data must be stored where the backup schedule is appropriate to the importance of the data, at the discretion of the user.

#### 4.2.d Critical

Critical data should be stored on a server that gets the most frequent backups (refer to the Backup Policy for additional information). Some type of system- or disk-level redundancy is encouraged.

#### 4.2.e Confidential

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

### 4.3 Data Transmission

The following guidelines apply to transmission of the different types of company data.

**4.3.a Personal**

There are no requirements for personal information.

**4.3.b Public**

There are no requirements for public information.

**4.3.c Operational**

No specific requirements apply to transmission of Operational Data, however, as a general rule, the data should not be transmitted unless necessary for business purposes.

**4.3.d Critical**

There are no requirements on transmission of critical data, unless the data in question is also considered operational or confidential, in which case the applicable policy statements would apply.

**4.3.e Confidential**

Confidential data must not be 1) transmitted outside NWN Carousel network without the use of strong encryption, 2) left on voicemail systems, either inside or outside NWN Carousel network.

**4.4 Data Destruction**

The following guidelines apply to the destruction of the different types of company data.

**4.4.a Personal**

There are no requirements for personal information.

**4.4.b Public**

There are no requirements for public information.

**4.4.c Operational**

There are no requirements for the destruction of Operational Data, though shredding is encouraged.

**4.4.d Critical**

There are no requirements for the destruction of Critical Data, though shredding is encouraged. If the data in question is also considered operational or confidential, the applicable policy statements would apply.

**4.4.e Confidential**

Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

Paper/documents: crosscut shredding is required. Storage media (CD's, DVD's): physical destruction is required. Hard Drives/Systems/Mobile Storage Media: at a minimum, data wiping must be used.

Simply reformatting a drive does not make the data unrecoverable. If wiping is used, NWN Carousel must use the most secure commercially available methods for data wiping. Alternatively, NWN Carousel has the option of physically destroying the storage media.

**4.5 Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

**4.6 Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

**5.0 Revision History**

Name	Date	Brief Description of Changes	Version
James Aiello	8/2/11	Reformatted Classification Policy	Version 1.1




James Aiello	10/31/11	Reformatted Classification Policy	Version 1.2
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.0
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.1
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

**6.0 Approval History**

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

**7.0 Review Cycle**

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	11/1/11	CIIMT	Completed
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NCI001-F <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>CONFIDENTIAL DATA POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

Confidential Data is typically the data that holds the most value to a company. Often, confidential data is valuable to others as well, and thus can carry greater risk than general company data. For these reasons, it is good practice to dictate security standards that relate specifically to confidential data.

## 2.0 Scope

The scope of this policy covers all company-confidential data, including sensitive customer information, regardless of location. Also covered by the policy are hardcopies of company data, such as printouts, faxes, notes, etc.

## 3.0 Goals

The purpose of this policy is to detail how confidential data, as identified by the Data Classification Policy, should be handled. This policy lays out standards for the use of confidential data, and outlines specific security controls to protect this data.

## 4.0 Policy

### 4.1 Treatment of Confidential Data

For clarity, the following sections on storage, transmission, and destruction of confidential data are restated from the Data Classification Policy.

#### 4.1.a Storage

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

#### 4.1.b Transmission

It is NWN Carousel preference that all confidential material be shared and transferred via strong encryption means only with employees, vendors and customers that require direct access to such information. It is understood that not all vendors and customers share a similar philosophy regarding the transmission of confidential material and all efforts should be made to utilize the highest level of security available for the sharing and transmission of confidential material

#### 4.1.c Destruction

Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: crosscut shredding is required.
- Storage media (CD's, DVD's): physical destruction is required.
- Hard Drives/Systems/Mobile Storage Media: at a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, NWN Carousel must use the most secure commercially available methods for data wiping. Alternatively, NWN Carousel has the option of physically destroying the storage media.

### 4.2 Use of Confidential Data

A successful confidential data policy is dependent on the users knowing and adhering to NWN Carousel standards involving the treatment of confidential data. The following applies to how users must interact with confidential data:

- Users must be advised of any confidential data they have been granted access. Such data should be marked or otherwise designated "confidential."
- Users must only access confidential data to perform his/her job function.
- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.
- Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to

- do his or her job or the action is approved by his or her supervisor.
- Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor.
- If confidential information is shared with third parties, such as contractors or vendors, a confidential information or non-disclosure agreement must govern the third parties' use of confidential information. Refer to NWN Carousel External Supplier Management Policy for additional guidance.

### **4.3 Security Controls for Confidential Data**

Confidential data requires additional security controls in order to ensure its integrity. NWN Carousel requires that the following guidelines are followed:

- **Strong Encryption.** Strong encryption must be used for confidential data transmitted external to NWN Carousel. If confidential data is stored on laptops or other mobile devices, it must be stored in encrypted form.
- **Network Segmentation.** Separating confidential data by network segmentation is strongly encouraged.
- **Authentication.** Strong passwords must be used for access to confidential data.
- **Physical Security.** Systems that contain confidential data should be reasonably secured.
- **Printing.** When printing confidential data users must use best efforts to ensure that the information is not viewed by others and destroyed when no longer required.
- **All system components that must go offsite for repair or replaced are sanitized of confidential state data.**
- **Faxing.** When faxing confidential data, users should use cover sheets that inform the recipient that the information is confidential. Fax machines that are regularly used for sending and/or receiving confidential data must be located in secured areas.
- **Emailing.** Confidential data must not be emailed outside NWN Carousel without the use of strong encryption. (Note: This does not include PERSONAL INFORMATION. Please see the Personal Information Policy for further reference, as NWN Carousel does NOT support the transmission of PERSONAL data across its email systems.)
- **Mailing.** If confidential information is sent outside NWN Carousel, it is recommended that the user use a service that requires a signature for receipt of that information.
- **Discussion.** When confidential information is discussed it should be done in non-public places, and where the discussion cannot be overheard.
- **Confidential data must be removed from documents unless its inclusion is absolutely necessary.**
- **Confidential data must never be stored on non-company-provided machines (i.e., home computers).**
- **If confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.**

### **4.4 Examples of Confidential Data**

The following list is not intended to be exhaustive, but should provide NWN Carousel with guidelines on what type of information is typically considered confidential. Confidential data can include:

- Employee or customer social security numbers or personal information
- Medical and healthcare information
- Electronic Protected Health Information (EPHI)
- Customer data
- Company financial data (if company is closely held)
- Sales forecasts
- Product and/or service plans, details, and schematics,
- Network diagrams and security configurations
- Communications about corporate legal matters
- Passwords
- Bank account information and routing numbers
- Payroll information
- Credit card information
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

### **4.5 Clear Desk Policy**

It is generally accepted that a clear desk is a sign of efficiency and effectiveness. A neat desk serves to keep confidential information secure, minimizes the risk of theft in the workplace and produces a positive image for guests and potential clients visiting our facilities. Therefore, it is each employee's responsibility to maintain a neat working environment by adhering to this Clear Desk Policy. The following are the minimum requirements for complying with the clear desk policy:

- All confidential data must be locked away when not at your desk per the Confidential Data Policy.

- All portable devices capable of storing data must be locked up out of sight at the end of the day. This includes laptops, external hard drives, flash memory sticks, CD's, DVD's etc.
- Employees are expected to clean and organize their desk at least once a week.

#### 4.6 **Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

#### 4.7 **Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

### 5.0 **Revision History**


Name	Date	Brief Description of Changes	Version
James Aiello	8/2/11	Reformatted Confidential Data Policy	Version 1.1
James Aiello	10/31/12	Audited Policy; Added Clean Desk Policy	Version 1.2
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.0
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.1
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.2
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.3
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

### 6.0 **Approval History**

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

### 7.0 **Review Cycle**

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	11/1/12	CIIMT	Completed
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-G <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>ELECTRONIC COMMUNICATIONS POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

Electronic Communications are an essential component of business communication; however it presents a particular set of challenges due to its potential to introduce a security threat to the network. Email & Instant Messaging can also have an effect on NWN Carousel liability by providing a written record of communications, so having a well thought out policy is essential. This Electronic Communications Policy outlines expectations for appropriate, safe, and effective use of the corporate electronic communication systems.

## 2.0 Scope

The scope of this policy includes NWN Carousel’ email & instant messaging systems, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. It covers all electronic communication sent from the system, as well as any external accounts accessed from NWN Carousel network.

## 3.0 Goals

The goal of this policy is to detail NWN Carousel usage guidelines for electronic communications. This policy will help NWN Carousel reduce risk of an email-related security incident, foster good business communications both internal and external to NWN Carousel, and provide for consistent and professional application of NWN Carousel communication principles.

## 4.0 Policy

### 4.1 Proper Use of Company Electronic Communication Systems

Users are asked to exercise common sense when using the corporate electronic communication systems. Additionally, the following applies to the proper use of NWN Carousel email system.

#### 4.1.a General Guidelines

Personal usage of company electronic communication systems is prohibited. Users should use corporate systems for business communications only.

- Personal usage of company electronic communication systems is prohibited. Users should use corporate systems for business communications only.
- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.
- The user is prohibited from forging email header information or attempting to impersonate another person.
- Instant Messaging is an insecure method of communication, and thus information that is considered confidential, personal or proprietary to NWN Carousel must not be sent via email, regardless of the recipient.
- It is company policy not to open attachments from unknown senders, or when such attachments are unexpected.
- The Email and Instant Messaging systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. NWN Carousel electronic communications systems are configured to block all messages both inbound and outbound that meet or exceed a 25 megabytes limit.
- Email systems were not designed to be file folder storage repositories and should not be treated as such. Storing and collecting historical information, emails and documents within your email account is not a NWN Carousel approved practice.
- Please note that the topics above may be covered in more detail in other sections of this policy.

#### 4.1.b Business Communications

NWN Carousel uses electronic communications as a vital medium for business operations. Users of the corporate electronic communications system are expected to check and respond to messages in a consistent and timely manner during business hours. Additionally, users are asked to recognize that any email sent from a company account reflects on NWN Carousel, and, as such, must be used with

professionalism and courtesy.

#### **4.1.c Instant Messaging**

Instant messaging provides a valuable form of communication in both a personal and professional setting. It should also be noted that Instant Messaging is an unsecure medium and that users are expected follow all applicable Information Security Policies, especially in regards to the disclosure of confidential data and it is with this in mind that all instant messaging is subject to monitoring by CSOIT.

#### **4.1.d Public Presence**

All employees are expected to utilize the presence features of the NWN Carousel standard instant messaging platform client to show their availability. This will prove especially useful for ensuring that you are not disrupted while assisting a customer or when working on a sensitive project.

#### **4.1.e Sending Email**

When using a company email account, email must be addressed and sent carefully. Users should keep in mind that NWN Carousel loses any control of email once it is sent external to NWN Carousel network. Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists to avoid inadvertent information disclosure to an unintended recipient. Careful use of email will help NWN Carousel avoid the unintentional disclosure of sensitive or non-public information.

#### **4.1.f Email Signature**

An email signature (contact information appended to the bottom of each outgoing email) is required for all emails sent from NWN Carousel email system. Instructions for setting up the standard company email signature can be found on SharePoint. Email signatures may not include personal messages (political, humorous, graphics, etc.).

#### **4.1.g Auto-Responders**

NWN Carousel requires the use of an auto-responder if the user will be out of the office for an entire business day or more. The auto-response should notify the sender that the user is out of the office, the date of the user's return, and whom the sender should contact if immediate assistance is required.

#### **4.1.h Mass Emailing**

NWN Carousel makes the distinction between the sending of mass emails and the sending of unsolicited email (spam). Mass emails may be useful for both sales and non-sales purposes (such as when communicating with NWN Carousel employees or customer base), and is allowed as the situation dictates. The sending of spam, on the other hand, is strictly prohibited.

It is NWN Carousel intention to comply with applicable laws governing the sending of mass emails. NWN Carousel requires that email sent to more than fifty (50) external recipients be sent with a 3<sup>rd</sup> party system to ensure that it does not impact NWN Carousel's email reputation score and must have the following characteristics:

- The email must contain instructions on how to unsubscribe from receiving future emails (a simple "reply to this message with UNSUBSCRIBE in the subject line" will do). Unsubscribe requests must be honored immediately.
- The email must contain a subject line relevant to the content.
- The email must contain contact information, including the full physical address, of the sender.
- The email must contain no intentionally misleading information (including the email header), blind redirects, or deceptive links.
- Note that emails sent to company employees, existing customers, or persons who have already inquired about NWN Carousel services are exempt from the above requirements.

Similarly, NWN Carousel does not condone the mass emailing of internal employees either. Exceptions to this rule are provided to business leaders and cases where clear communications are needed across the organization. While a marketing system need not be used when sending internal emails, users will be systematically limited to the number of recipients they are able to send to prevent mass mailings.

#### **4.1.i Opening Attachments**

Users must use care when opening attachments whether from email or an Instant Messaging platform. Viruses, Trojans, and other malware can be easily delivered as an email attachment. Users should:

- Never open unexpected attachments.

- Never open email attachments from unknown sources.
- Never click links within email messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially formatted emails can hide a malicious URL.
- NWN Carousel may use methods to block what it considers to be dangerous or emails or strip potentially harmful email attachments, as it deems necessary.

#### **4.1.j Monitoring and Privacy**

Users should expect no privacy when using the corporate network or company resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. NWN Carousel reserves the right to monitor any and all use of the computer network. To ensure compliance with company policies this may include the interception and review of any messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

#### **4.1.k Company Ownership of Electronic Communications**

Users should be advised that NWN Carousel owns and maintains all legal rights to its electronic communication systems and network, and thusly, any message passing through these systems is owned by NWN Carousel and it may be subject to use for purposes not be anticipated by the user. Keep in mind that electronic communication may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the user should be advised that email sent to or from certain public or governmental entities may be considered public record.

#### **4.1.l Contents of Received Emails**

Users must understand that the contents of external inbound email may contain material that the user finds offensive. If unsolicited email becomes a problem, NWN Carousel may attempt to reduce the amount of this email that the users receive, however no solution will be 100% effective. The best course of action is to not open emails that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email, or believes that it contains illegal content, he or she should notify his or her supervisor and/or open a ticket with the NWN Carousel help desk.

#### **4.1.m Access to Email from Mobile Phones**

NWN Carousel allows mobile device access to email based upon role responsibilities. It is required devices accessing corporate email services are password protected from the lock screen. CSOIT reserves the right to remotely apply administrative controls to any device accessing corporate email.

### **4.2 External and/or Personal Email Accounts**

NWN Carousel recognizes that users may have personal email accounts in addition to their company-provided account. The following sections apply to non-company provided email accounts:

#### **4.2.a Use for Company Business**

Users must use the corporate email system for all business-related email. Users are prohibited from sending business email from a non-company-provided email account.

#### **4.2.b Use for Personal Reasons**

Users are required to use a non-company-provided (personal) email account for all non-business communications. The corporate email system is for corporate communications only. Users must follow applicable policies regarding the access of non-company-provided accounts from NWN Carousel network.

### **4.3 Confidential Data and Electronic Communications**

The following sections relate to confidential data and email:

#### **4.3.a Passwords**

As with any company passwords, passwords used to access email accounts must be kept confidential and used in adherence with the Password Policy. At the discretion of the CSOIT Management, NWN Carousel may further secure email with certificates; two factor authentication, or another security mechanism.

#### **4.3.b Transferring Confidential Data**

Email is an insecure means of communication. Users should think of email as they would a postcard, which, like email, can be intercepted and read on the way to its intended recipient.

NWN Carousel requires that any email containing confidential or personal information, regardless of whether the recipient is internal or external to NWN Carousel network, be encrypted using commercial-grade, strong encryption. Care must also be used with sending Confidential Data via Instant Messaging.

Further guidance on the treatment of confidential information exists in NWN Carousel Confidential Data Policy. If information contained in the Confidential Data Policy conflicts with this policy, the Confidential Data Policy will apply.

#### **4.4 Company Administration of Electronic Communications**

NWN Carousel will use its best effort to administer NWN Carousel Electronic Communications system in a manner that allows the user to both be productive while working as well as reduce the risk of a security incident.

##### **4.4.a Filtering of Email**

A good way to mitigate risk from email is to filter it before it reaches the user so that the user receives only safe, business-related messages. For this reason, NWN Carousel will filter email at the Internet gateway and/or the mail server, in an attempt to filter out spam, viruses, or other messages that may be deemed contrary to this policy or a potential risk to the NWN Carousel network security. No method of email filtering is 100% effective, so the user is asked additionally to be cognizant of this policy and use common sense when opening emails.

Additionally, many email and/or anti-malware programs will identify and quarantine emails that it deems suspicious. This functionality may or may not be used at the discretion of the IT Manager.

##### **4.4.b Email Deletion**

Users are encouraged to delete email periodically when the email is no longer needed for business purposes. The goal of this policy is to keep the size of the user's email account manageable, and reduce the burden on NWN Carousel to store and backup unnecessary email messages.

However, users are strictly forbidden from deleting email in an attempt to hide a violation of this or another company policy. Further, email must not be deleted when there is an active investigation or litigation where that email may be relevant.

##### **4.4.c Retention and Backup**

Electronic communications must be retained and backed up in accordance with the applicable policies, which may include but are not limited to the: Data Classification Policy, Confidential Data Policy, Backup Policy, and Retention Policy.

Unless otherwise indicated, for the purposes of backup and retention, email should be considered operational data.

##### **4.4.d Address Format**

Email addresses must be constructed in a standard format in order to maintain consistency across NWN Carousel. The approved address formats are:

- FirstinitialLastname
- FirstinitialMiddleinitialLastname

##### **4.4.e Email Aliases**

Often the use of an email alias, which is a generic address that forwards email to a user account, is a good idea when the email address needs to be in the public domain, such as on the Internet. Aliases reduce the exposure of unnecessary information, such as the address format for company email, as well as (often) the names of company employees who handle certain functions. Keeping this information private can decrease risk by reducing the chances of a social engineering attack.

A few examples of commonly used email aliases are:

- sales@companydomain.com
- techsupport@companydomain.com
- pr@companydomain.com
- info@companydomain.com

NWN Carousel requires the use of email aliases in all situations where an email address will be exposed to, or reachable by, the general public.

##### **4.4.f Account Activation**

Electronic communication accounts will be set up for each user determined to have a business need to



send and receive on the corporate systems. Accounts will be set up at the time a new hire starts with NWN Carousel, or when a promotion or change in work responsibilities for an existing employee creates a need.

#### **4.4.g Account Termination**

When a user leaves NWN Carousel, or his or her access is officially terminated for another reason, NWN Carousel will disable the user's access to the account by password change, disabling the accounts, or another method. NWN Carousel is under no obligation to block an email account from receiving email, and may continue to forward inbound email sent to that account to another user, or set up an auto-response to notify the sender that the user is no longer employed by NWN Carousel.

#### **4.4.h Storage Limits**

As part of the email service, email storage may be provided on company servers or other devices. The email account storage size must be limited to what is reasonable for each employee, at the determination of CSOIT. Storage limits may vary by employee or position within NWN Carousel.

### **4.5 Prohibited Actions**

The following actions shall constitute unacceptable use of the corporate electronic communication systems. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate systems to:

- Send any information that is illegal under applicable laws.
- Access another user's account without
  - The knowledge or permission of that user - which should only occur in extreme circumstances
  - The approval of company executives in the case of an investigation
  - such access constitutes a function of the employee's normal job responsibilities.
- Send any communication that may cause embarrassment, damage to reputation, or other harm to NWN Carousel.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Send communications that cause disruption to the workplace environment or create a hostile workplace. This includes sending messages that are intentionally inflammatory, or that include information not conducive to a professional working atmosphere.
- Make fraudulent offers for products or services.
- Attempt to impersonate another person or forge an email header.
- Send spam, solicitations, chain letters, or pyramid schemes.
- Knowingly misrepresent NWN Carousel capabilities, business practices, warranties, pricing, or policies.
- Conduct non-company-related business.

NWN Carousel may take steps to report and prosecute violations of this policy, in accordance with company standards and applicable laws.

### **4.6 Data Leakage**

Data can leave the network in a number of ways. Often this occurs unintentionally by a user with good intentions. For this reason, email poses a particular challenge to NWN Carousel control of its data.

Unauthorized distribution of company data, confidential or otherwise, to external email accounts for the purpose of saving this data external to company systems is prohibited. If a user needs access to information from external systems (such as from home or while traveling), that user should notify his or her supervisor rather than emailing the data to a personal account or otherwise removing it from company systems.

NWN Carousel may employ data loss prevention techniques to protect against leakage of confidential data at the discretion of CSOIT.

### **4.7 Sending Large Emails**

Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. NWN Carousel asks that the user limit email attachments to 25Mb or less.

The user is further asked to recognize the additive effect of large email attachments when sent to multiple recipients, and use restraint when sending large files to more than one person.

### **4.8 Monitoring & Privacy Rights**

Users should have no expectation of privacy when using the corporate electronic communication systems. Such use may include, but is not limited to: transmission and storage of files, data, email and messages. CSOIT is continuously monitoring the corporate network, and by extent, all devices connected to it. This monitoring is done to ensure the integrity of the network and to ensure compliance with established security policies. CSOIT

may access any and all information technology resources at any time in accordance with company Information Security Policies.

#### 4.9 **Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

#### 4.10 **Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

### 5.0 **Revision History**


Name	Date	Brief Description of Changes	Version
James Aiello	7/25/11	Reformatted Email Policy	Version 1.1
James Aiello	10/31/11	Reformatted Email Policy	Version 1.2
James Aiello	3/21/13	Audited Email Policy; Changed Name to “Electronic Communications Policy”	Version 2.0
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.1
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.2
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

### 6.0 **Approval History**

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methe	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

### 7.0 **Review Cycle**

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	06/01/13	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-H <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>EMPLOYEE ADMINISTRATION POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

To provide a clear and concise overview of the policies that apply to the end user lifecycle from hire to separation.

## 2.0 Scope

This policy applies to all employee, contractor, guest or other individual who requires access to corporate Information Technology resources including, but not limited to, production & lab computer systems, email, networks, and the Corporate Network.

## 3.0 Goal

To ensure the accurate and timely management of all user accounts across all NWN Carousel systems.

## 4.0 Policy

### 4.1 Employee Management Requirements

The following items are the corporate policy statements for adding new users, changing existing user access, and terminating users:

- Requests for adding access for personnel accounts will be accomplished by the hiring manager submitting a ticket for Access Request Form, which HR needs to approve if access to sensitive customer information is required.
- Requests for changing or revising existing user access for individual accounts must be submitted through the Access Request Form by the Manager which HR needs to approve if access to sensitive customer information is required.
- Requests for terminating access will be accomplished by the manager following the defined HR process for employee termination.
- Additional access beyond the normal on-boarding access needs to be submitted as a ticket by the hiring manager.
- Prior to gaining access to the company or customer computing resources, all users must certify (in writing) that they have read and understood the company security policy statements.
- All user requests must be approved by the hiring manager.
- Managers must ensure that employees have completed all required security training. HR will ensure that this training is complete before access to sensitive customer information is granted.
- Approve level of access as appropriate, but not exceeding the access required for the user to perform their duties in accordance with NWN Carousel’s policies of least required access.

### 4.2 Employee Screening

To ensure the security of our customer data, all employees and contractors will undergo a background screening prior to being provided access to confidential systems.

- Initial screening must be conducted prior to authorizing access to information systems or data, including staff transfers.
- The screening process must include all elements to comply with existing regulations, and must be reviewed at least annually to ensure that it remains relevant and compliant.
- The results of the screening process must be recorded in accordance with existing records retention policies, and regulatory requirements.

### 4.3 Onboarding

This section provides a guideline for the necessary steps in the event of onboarding a new employee within NWN Carousel.

- A new hire ticket will be submitted by HR
- Once the ticket is received and assigned the CSOIT point of contact will:
  - Start an Onboarding Process for the new employee
  - Verify new employee technology profile with hiring manager
  - Verify start date for new employee
  - Pull equipment and stage for preparation

- Based on technologies to be issued, start profile build and work with associated CSOIT team members to complete “Onboarding checklist” form
- Coordinate with new employee for equipment pick up or shipment
- Close New Hire Ticket

#### 4.4 **Employee Transfer**

This section provides a guideline for the necessary steps in the event of an employee transfer within NWN Carousel.

- A change request ticket will be submitted by HR
- Once the ticket is received and assigned the CSOIT point of contact will:
  - Verify the employee changes with supervisor or manager that the employee reports to
  - Verify the effective date for the employee transfer
  - Review and verify any technologies that may need to be updated,
    - Returned or canceled, and provided for the new position by
    - Pulling a copy of their current technology profile and asset form
  - Complete employee transfer checklist
  - Coordinate with employee for equipment pick up or shipment
  - Set up training for new technologies
  - Close change request ticket

#### 4.5 **Termination**

This section will provides an overview of the process for when an employee leaves the company. These procedures have been written to ensure the confidentiality of business information and to ensure a smooth transition for the business. All terminations must be thoroughly documented using the submitted Separation Request from Human Resources.

- A termination request ticket will be submitted by HR
- Once the ticket is received and assigned the CSOIT point of contact will:
  - Start an Employee Termination Process for the employee
  - And commence with *Immediate actions*
  - Follow up with *Within First Week actions*
  - Follow up with *After 60 Days actions*
  - Close Employee Termination Ticket

#### 4.6 **Monitoring & Privacy Rights**

Users should have no expectation of privacy when using the corporate electronic communication systems. Such use may include, but is not limited to: transmission and storage of files, data, email and messages. CSOIT is continuously monitoring the corporate network, and by extent, all devices connected to it. This monitoring is done to ensure the integrity of the network and to ensure compliance with established security polices. CSOIT may access any and all information technology resources at any time in accordance with company Information Security Policies.

#### 4.7 **Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

### 5.0 **Revision History**

Name	Date	Brief Description of Changes	Version
James Aiello	10/10/21	Created Employee Management Policy	Version 1.0
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1


### 6.0 **Approval History**

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23

Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

**7.0 Review Cycle**

<b>Review Cycle</b>	<b>Scheduled Review Date</b>	<b>Reviewer</b>	<b>Status-Action Needed</b>
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-I <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>ENCRYPTION POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

Encryption, also known as cryptography, can be used to secure data while it is stored or being transmitted. It is a powerful tool when applied and managed correctly. As the amount of data NWN Carousel must store digitally increases, the use of encryption must be defined and consistently implemented in order ensure that the security potential of this technology is realized.

## 2.0 Scope

This Encryption Policy covers all data stored on or transmitted across corporate systems.

## 3.0 Goals

The goal of this policy is to outline NWN Carousel standards for use of encryption technology so that it is used securely and managed appropriately. Many policies touch on encryption of data so this policy does not cover what data is to be encrypted, but rather how encryption is to be implemented and controlled.

## 4.0 Policy

### 4.1 Applicability of Encryption

#### 4.1.a Data while stored.

This includes any data located on company-owned or company-provided systems, devices, media, etc. Examples of encryption options for stored data include:

- Whole disk encryption
- Encryption of partitions/files
- Encryption of disk drives
- Encryption of personal storage media/USB drives
- Encryption of backups
- Encryption of data generated by applications

#### 4.1.b Data while transmitted.

This includes any data sent across NWN Carousel network, or any data sent to or from a company-owned or company-provided system. Types of transmitted data that can be encrypted include:

- VPN tunnels
- Remote access sessions
- Web applications
- Email and email attachments
- Remote desktop access
- Communications with applications/databases

### 4.2 Encryption Key Management

Key management is critical to the success of an implementation of encryption technology. The following guidelines apply to NWN Carousel encryption keys and key management:

- Management of keys must ensure that data is available for decryption when needed
- Keys must be backed up
- Keys must be locked up
- Keys must never be transmitted in clear text
- Keys are confidential data
- Keys must not be shared
- Physical key generation materials must be destroyed within 5 business days.
- Keys must be used and changed in accordance with the password policy.
- When user encryption is employed, the minimum key length is 10 characters.

### 4.3 Acceptable Encryption Algorithms

Only the strongest types of generally accepted, non-proprietary encryption algorithms are allowed, such as AES

or 3DES. Acceptable algorithms should be reevaluated as encryption technology changes.

Use of proprietary encryption is specifically forbidden since it has not been subjected to public inspection and its security cannot be assured.

#### 4.4 Legal Use

Some governments have regulations applying to the use and import/export of encryption technology. NWN Carousel must conform to encryption regulations of the local or applicable government.

NWN Carousel specifically forbids the use of encryption to hide illegal, immoral, or unethical acts. Anyone doing so is in violation of this policy and will face immediate consequences per the Enforcement section of this document.

#### 5.0 Revision History


Name	Date	Brief Description of Changes	Version
James Aiello	8/2/11	Reformatted Encryption Policy	Version 1.1
James Aiello	10/31/11	Audited Encryption Policy	Version 1.2
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.0
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.1
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.2
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.3
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

#### 6.0 Approval History

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

#### 7.0 Review Cycle

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	10/31/11	CIIMT	Completed
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-J <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>EXTERNAL SUPPLIER MANAGEMENT POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

The efficient and secure management of external suppliers is critical to ensuring the integrity and security of NWN Carousel’s customers information.

## 2.0 Scope

This Policy covers all aspects of management for our external suppliers including contractual, risk management, information security, and network connectivity.

## 3.0 Goals

The goal of this policy is to document the comprehensive set of controls in place to manage all External Suppliers.

## 4.0 Policy

### 4.1 Evaluating a Provider

Once the decision to utilize a vendor has been made, selecting the appropriate provider is critical to the success of the endeavor. Due diligence reviews must always be performed prior to a provider being selected. Due diligence review must include an evaluation of the provider's ability to perform the requested services, and must specifically cover the following areas:

- Technical ability of the provider
- Ability to deliver the service
- Experience of the provider
- Security state and related certifications
  - Security Governance
  - Compliance
  - Access Management
  - System Management
  - Network Management
  - Business Continuity & Disaster Recovery
- Reputation of the provider
- Policies and procedures related to the service
- Financial strength of the provider
- Service Level Agreements related to the service

If the outsourced service will involve the provider having access to, or storing NWN Carousel confidential information, due diligence must cover the provider's security controls for access to the confidential information utilizing NWN Carousels vendor analysis tool.

### 4.2 Contracts

All outsourced Information and Technology Management services must be governed by a legal contract, with an original of the executed contract maintained by NWN Carousel.

Contracts must:

- Cover a specified time period
- Specify exact pricing for the services
- Specify how the provider will treat confidential information
- Include a non-disclosure agreement
- Specify services to be provided, including Service Level Agreements and penalties for missing the levels
- Allow for cancellation if contractual terms are not met
- Specify standards for subcontracting of the services and reassignment of contract
- Cover liability issues
- Describe how and where to handle contractual disputes

### 4.3 Security Controls

The outsourcing contract must provide a mechanism for secure information exchange with the service provider.



This will vary with the type of service being outsourced, but may include remote access, VPN, or encrypted file exchange.

NWN Carousel and provider must also maintain a mechanism for verifying the identity of the other party and confirming changes to the service. This will prevent an attacker from using social engineering tactics to gain access to company data.

**4.3.a External Supplier Access to Sensitive Information**

The provider must be given the least amount of network, system, and/or data access required to perform the contracted services. This access must follow applicable policies and be periodically audited. Vendors with access to sensitive information (PHI, PII, Confidential Data, etc.) must agree to applicable legal statutes in order to be provided with access to said information. All contractual controls placed upon Carousel by our customers will be passed down to applicable vendors including legal language and security training.

**4.3.b Applicability of Third Party Connection Policy**

For further details on the security controls in place for Third Party Connections into NWN Carousel resources, please refer to the Third Party Connection Policy contained within the Information Security Manual.

**4.4 Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

**4.5 Security Compliance**

In order to ensure compliance with NWN Carousel Security objectives, key vendors will have a Risk Assessment performed annually against their security controls. Deficiencies will be notated within the Risk Management Register and tracked for remediation.

**4.6 Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

**5.0 Revision History**

Name	Date	Brief Description of Changes	Version
James Aiello	7/15/11	Reformatted Outsourcing Policy	Version 1.1
James Aiello	10/31/11	Reformatted Outsourcing Policy	Version 1.2
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.0
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.1
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.2
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.3
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1


**6.0 Approval History**

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23

NWN Carousel Security Committee		v3.1	5/19/23
---------------------------------	--	------	---------

**7.0 Review Cycle**

<b>Review Cycle</b>	<b>Scheduled Review Date</b>	<b>Reviewer</b>	<b>Status-Action Needed</b>
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-K <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>GUEST WIRELESS NETWORK POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

NWN Carousel understands the value of its guests' time. This is why access to a secure wireless network is provided as a courtesy to guests. This Guest Wireless Network Policy outlines NWN Carousel policies regarding access to the Guest Wireless Network.

## 2.0 Scope

This policy pertains to any visitor to a NWN Carousel facility wishing to access an outbound internet connection through the Guest Wireless Network. The scope of this policy does not include guests accessing wireless broadband accounts directly through a cellular carrier or third party where the traffic does not traverse NWN Carousel network or anyone needing access to the internal network. Contractors and vendors needing access to NWN Carousel' Internal Network should refer to the Network Access Policy for the correct procedure to request access.

## 3.0 Goals

The goal of this document is to outline the policies for accessing the NWN Carousel Guest Wireless Network. The successful implementation of these policies will allow guests access to a secure Internet connection while ensuring the security of the internal network and compliance with Information Technology Security Standards.

## 4.0 Policy

### 4.1 Guest Access

Access to a secure Guest Wireless account is provided by NWN Carousel to its clients, guests and visitors for the purpose of accessing the internet. In order to maintain the security of the network, login information will be changed monthly by CSOIT and only disseminated to approved individuals. Access to this connection is regulated and all guests must register with a NWN Carousel representative to receive a user name and password for access. Guests requesting access to NWN Carousel Internal Network will be evaluated and provided for in accordance with the Network Access Policy. This process will involve management approval if the request is non-standard.

### 4.2 Restrictions on Guest Access

Guest will only be provided with access to the Internet through the NWN Carousel Guest Wireless Network. All requests for hardwire access by a guest will be denied. NWN Carousel will evaluate the need of each guest and provide further access only if there is a business need to do so. Employees are reminded that the guest network is intended for guests only and are requested to refrain from attempting to access this network.

### 4.3 Monitoring & Privacy Rights

Guests should be aware that NWN Carousel is continuously monitoring all networks and connections that comprise the NWN Carousel Corporate Network, and by extent, devices logged into the guest wireless network. This monitoring is done to ensure the integrity of the network and to ensure compliance with established security policies. CSOIT may access any and all information technology resources at any time in accordance with company Information Security Policies and further reserves the right to block any devices that may pose a risk to the network.

### 4.4 Guest Access Infrastructure Requirements

Best practices dictate that guest access be kept separate, either logically or physically, from the corporate network. At a minimum, guest access must be logically separated from NWN Carousel network via a De Militarized Zone (DMZ), firewall, or other access controls. This is done because neither guests nor their devices have undergone the same amount of scrutiny as assets allowed on NWN Carousel Corporate Network.

### 4.5 Audits

The Guest Wireless Network must be audited yearly to ensure that all policies are being followed. Specific audit points should include: location of access points, signal strength, SSID, use of encryption and proper guest interface.

### 4.6 Applicability of Other Policies

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

#### 4.7 **Enforcement**

This policy will be enforced by the CSOIT and the Executive Team. Violations may result in disciplinary action, which may include being asked to leave the premises or a restriction of access. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

#### 5.0 **Revision History**


Name	Date	Brief Description of Changes	Version
James Aiello	08/26/11	Reformatted Guest Access Policy	Version 1.1
James Aiello	10/31/11	Reformatted Guest Access Policy	Version 1.2
James Aiello	12/1/11	Performed CIIMT Audit	Version 2.0
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.1
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.2
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

#### 6.0 **Approval History**

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methe	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

#### 7.0 **Review Cycle**

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	12/1/11	CIIMT	Completed
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/16	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-L <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>INCIDENT RESPONSE POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

A security incident can come in many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data. A well-thought-out Incident Response Policy is critical to successful recovery from an incident. This Incident Response Policy covers all incidents that may affect the security and integrity of NWN Carousel information assets, and outlines steps to take in the event of such an incident.

## 2.0 Scope

The scope of this policy covers all information assets owned or provided by NWN Carousel, whether they reside on the corporate network or elsewhere.

## 3.0 Goals

This policy is intended to ensure that NWN Carousel is prepared if a security incident were to occur. It details exactly what must occur if an incident is suspected, covering both electronic and physical security incidents. Note that this policy is not intended to provide a substitute for legal advice, and approaches the topic from a security practices perspective.

## 4.0 Policy

### 4.1 Types of Incidents

A security incident, as it relates to NWN Carousel information assets, can take one of two forms. For the purposes of this policy a security incident is defined as one of the following:

#### 4.1.a Electronic:

This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes, to a virus outbreak, to a suspected Trojan or malware infection.

#### 4.1.b Physical:

A physical IT security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain company information.

### 4.2 Incident Response Plan

Outside of this Policy, NWN Carousel will keep an Incident Response plan in place and updated as a runbook for any incident described within. Said Incident Response plan will be reviewed and tested annually in accordance with Information Security best practices. Due to the confidential nature of the information contained within, this Response Plan is not available for dissemination outside of the NWN Carousel.

### 4.3 Reporting of Security Incident

All security incidents must be reported to CSOIT as soon as an employee becomes aware that there might be a problem. Incidents can be reported by ticket or by contacting CSOIT directly.

### 4.4 Preparation

Work done prior to a security incident is arguably more important than work done after an incident is discovered. The most important preparation work, obviously, is maintaining good security controls that will prevent or limit damage in the event of an incident. These technical tools include firewalls, intrusion detection systems, authentication, and encryption; and non-technical tools such as good physical security for laptops and mobile devices.

NWN Carousel reviews industry and governmental regulations that dictate how we must respond to a security incident (specifically, loss of customer data), and ensure that its incident response plans adhere to these regulations.

### 4.5 Confidentiality

All information related to an electronic or physical security incident must be treated as confidential information

until the incident is fully contained. This will serve both to protect employees' reputations (if an incident is due to an error, negligence, or carelessness), and to control the release of information to the media and/or customers.

## **4.6 Electronic Incidents**

When an electronic incident is suspected, NWN Carousel goal is to recover as quickly as possible, limit the damage done, secure the network, and preserve evidence of the incident. The following steps should be taken in order:

1. Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.
2. Disable the compromised account(s) as appropriate.
3. Report the incident to the IT Manager.
4. Physically secure the compromised system.
5. Create a detailed event log documenting each step taken during this process.
6. Determine how the attacker gained access and disable this access.
7. Rebuild the system using new hardware.
8. Restore any needed data from the last known good backup and put the system back online.
9. Take actions, as possible, to ensure that the vulnerability (or similar vulnerabilities) will not reappear.
10. Notify applicable authorities if prosecution is desired and possible based on the evidence collected.
11. Reflect on the incident. What can be learned? How did the Incident Response team perform? Was the policy adequate? What could be done differently?
12. Perform a vulnerability assessment as a way to spot any other vulnerabilities before they can be exploited.

## **4.7 Physical Incidents**

Physical security incidents are challenging, since often the only actions that can be taken to mitigate the incident must be done in advance. This makes preparation critical. One of the best ways to prepare is to mandate the use of strong encryption to secure data on mobile devices. Applicable policies, such as those covering encryption and confidential data, should be reviewed.

Physical security incidents are most likely the result of a random theft or inadvertent loss by a user, but they must be treated as if they were targeted at NWN Carousel.

NWN Carousel must assume that such a loss will occur at some point, and periodically survey a random sampling of laptops and mobile devices to determine the risk if one were to be lost or stolen.

### **4.7.a Response**

Establish the severity of the incident by determining the data stored on the missing device. This can often be done by referring to a recent backup of the device. Two important questions must be answered:

1. Was confidential data involved?
  - a. If not, refer to "Loss Contained" below.
  - b. If confidential data was involved, refer to "Data Loss Suspected" below.
2. Was strong encryption used?
  - a. If strong encryption was used, refer to "Loss Contained" below.
  - b. If not, refer to "Data Loss Suspected" below.

### **4.7.b Loss Contained**

First, change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Notify the IT Manager. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities if a theft has occurred.

### **4.7.c Data Loss Suspected**

First, notify the executive team, legal counsel, and/or public relations group so that each team can evaluate and prepare a response in their area.

Change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities as needed if a theft has occurred and follow disclosure guidelines specified in the notification section.

Review procedures to ensure that risk of future incidents is reduced by implementing stronger physical security controls.

## **4.8 Notification**

If an electronic or physical security incident is suspected to have resulted in the loss of third-party/customer data,

notification of the public or affected entities should occur. First this must be discussed with executive team and legal counsel to determine an appropriate course of action. If notification is deemed an appropriate course of action, it should occur in an organized and consistent manner.

#### **4.9 Event Logging**

All security incidents must be logged and stored in accordance with business standards. These logs will be kept by CSOIT and reviewed on a regular basis during the risk assessment process.

#### **4.10 Managing Risk**

Managing risk of a security incident or data loss is the primary reason to create and maintain a comprehensive security policy. Risks can come in many forms: electronic risks like data corruption, computer viruses, hackers, or malicious users; or physical risks such as loss/theft of a device, hardware failure, fire, or a natural disaster. Protecting critical data and systems from these risks is of paramount importance to NWN Carousel.

##### **4.10.a Risk Assessment**

As part of the risk management process, NWN Carousel must conduct an accurate and thorough assessment of the potential risks (man-made and natural) and any vulnerabilities to the confidentiality, integrity, and availability of NWN Carousel critical or confidential information. An assessment must be thorough, can be performed by company personnel or external consultants (or both), and must be well documented.

##### **4.10.b Risk Management Program**

A formal risk management program must be implemented to cover any risks known to NWN Carousel (which should be identified through a risk assessment), and insure that reasonable security measures are in place to mitigate any identified risks to a level that will ensure the continued security of NWN Carousel confidential and critical data.

#### **4.11 Breach of Personally Identifiable Information (PII)**

The Breach of any Personally Identifiable Information (PII), including Protected Health Information (PHI), is a very serious matter and must be handled with the upmost care and expediency. For more information, please refer to the Privacy Policy. The following section is copied from the Privacy Policy in regards to our responsibilities in the event of a Breach of PHI:

##### **4.11.a Customer Notification**

The term “Breach” means the acquisition, access, use, or disclosure of Personally Identifiable Information by a covered entity and includes information in both physical and electronic form. NWN Carousel shall report to the customer in writing of any Breach of PII or PHI that it becomes aware within 48 hours of discovery unless otherwise contractually agreed upon. Written notice shall contain:

- The date of discovery of the Breach;
- A listing of the identification of individuals and/or classes of individuals who are subject to the Breach
- A general description of the nature of the Breach.

It is the sole responsibility of the customer to notify the impacted individuals of any breach of PII or PHI. At no time, will NWN Carousel contact or speak directly to any individuals who are the subject of any Breach. NWN Carousel shall cooperate with customers to assist in notification and any details pertaining to any Breach of information.

#### **4.12 Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

#### **4.13 Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

### **5.0 Revision History**

Name	Date	Brief Description of Changes	Version
------	------	------------------------------	---------

James Aiello	08/26/11	Reformatted Incident Response Policy	Version 1.1
James Aiello	10/31/11	Reformatted Incident Response Policy	Version 1.2
James Aiello	06/04/13	Audited Incident Response Policy	Version 2.0
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.1
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.2
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1


## 6.0 Approval History

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methe	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

## 7.0 Review Cycle

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	06/01/13	CIIMT	Completed
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled



	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-M <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>MOBILE DEVICE POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

Generally speaking, a mobile workforce is more flexible and productive and for this reason, business use of mobile devices is growing. However, as these devices become vital tools to the workforce, more and more sensitive data is stored on them, and thus the risk associated with their use is growing. Special consideration must be given to the security of mobile devices. The purpose of this policy is to specify company standards for the use and security of mobile devices.

## 2.0 Scope

The Mobile Device Policy applies to company data as it relates to mobile devices that are capable of storing such data, including, but not limited to notebooks, tablets, PDAs, smartphones, and USB drives. This policy covers any mobile device capable of coming into contact with company data. Please note that company standards as they pertain to computers, including laptops, are covered in the Acceptable Use Policy.

## 3.0 Goals

The goal of this policy is to provide specific company standards for the use and security of mobile devices as related to company data.

## 4.0 Policy

### 4.1 General Guidelines

The following guidelines apply to the use of mobile devices:

- Loss, Theft, or any other security incident related to a company-provided mobile device must be reported promptly to CSOIT.
- Confidential data should not be stored on mobile devices unless it is absolutely necessary. If confidential data is stored on a mobile device it must be appropriately secured and comply with the Confidential Data policy (i.e. full device encryption).
- Data stored on mobile devices must be securely disposed of in accordance with the Data Classification Policy.

### 4.2 Mobile Device Management

In today's world of Smartphones, tablets and small form laptops, the delineation of technology has become blurry. For this reason, CSOIT will act as the Point of Contact for all issues involving Mobile Devices. All devices attempting to connect to the NWN Carousel network must meet the requirements set forth in the Network Access and Authentication Policy.

### 4.3 Data Security

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting company data. The following sections specify NWN Carousel requirements for data security as it relates to mobile devices:

#### 4.3.a Laptops

At a minimum, confidential company data will be stored on an encrypted partition. Whole disk encryption will be considered if the data is especially sensitive. Laptops must require a username and password or biometrics for login. Please refer to the Password Policy for the correct formation for passwords. Personal computers are not allowed to connect to NWN Carousel's Corporate Network.

#### 4.3.b Smartphones/Tablets

Use of encryption is not required on smartphones or tablets but it encouraged if data stored on the device is especially sensitive. Smartphones and tablets must require a password or biometrics for login. Please refer to the Password Policy for the correct formation for passwords. All devices that connect to the Corporate Network must allow CSOIT administrative privileges in order to ensure that the device complies with our technology standards.

#### **4.3.c Mobile Storage Media**

This section covers any USB drive, flash drive, memory stick or any other mobile data storage medium. Encryption is required on these devices when they contain customer or company information.

#### **4.3.d Portable Media Players**

No company data can be stored on personal media players.

#### **4.3.e Other Mobile Devices**

Unless specifically addressed by this policy, storing company data on any other mobile device, or connecting personal devices to the company network, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to CSOIT Management.

### **4.4 Device Protection**

NWN Carousel utilizes multiple forms of protection for all corporate owned mobile devices. At a minimum, devices will be bound to the NWN Carousel domain to ensure all applicable GPOs are pushed to the device along with a version of the approved Anti-Malware/Virus protection.

### **4.5 Connecting to Unsecured Networks**

Users must not connect to any outside network without a secure, up-to-date software firewall configured on the Mobile Device. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of NWN Carousel.

### **4.6 Personal Mobile Devices**

As stated above, mobile devices can greatly enhance a workforce's productivity. However, the introduction of personal mobile devices into the workplace does pose a risk to the security of data and the network infrastructure of NWN Carousel. With this in mind, Personal Mobile Devices that connect to the corporate network must allow CSOIT the ability to manage the device, including the wiping of all data on the device in the event of the loss of the device or separation from the company. For more information on connectivity please refer to the Network Access Policy.

### **4.7 Replacement Device Request**

All requests for a replacement device must be submitted by ticket to CSOIT. A CSOIT technician must speak with the user about the reasons for their request before a final determination is made. In circumstances where an employee has demonstrated continual abuse or neglect with NWN Carousel technology, CSOIT reserves the right to initiate administrative action. This action could include, but is not limited to, issuance of low-cost technology alternative, refusal to issue technology, notifying the employee's manager for remediation, notifying Human Resources for documentation within the employee's record, or termination. In the case of an employee being denied technology, the employee may expense the cost of usage but not that of a new device. All complaints of technology neglect will be reviewed by CSOIT on a case-by-case basis.

### **4.8 Mobile Device Monitoring**

NWN Carousel reserves the right to monitor any device that connects to the company's network to ensure compliance with all pertinent policies and standards of use.

### **4.9 Mobile Devices and Motor Vehicles**

Despite the fact that we work in a fast paced environment, NWN Carousel insists that all local laws and ordinances regarding the use of mobile devices while driving be adhered to. NWN Carousel also strongly encourages the use of hands free devices while driving for all employees, regardless of the local ordinances.

### **4.10 End of Employment**

When a user's employment comes to an end at NWN Carousel, they are required to return all issued devices to CSOIT or Human Resources within 10 business days.

### **4.11 Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

### **4.12 Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or

intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

## 5.0 Revision History


Name	Date	Brief Description of Changes	Version
James Aiello	07/20/11	Reformatted Mobile Device Policy	Version 1.1
James Aiello	10/31/11	Reformatted Mobile Device Policy	Version 1.2
James Aiello	9/29/14	Edited Mobile Device Policy per CIIMT Audit	Version 2.0
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.1
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.2
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

## 6.0 Approval History

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methe	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

## 7.0 Review Cycle

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	9/29/14	CIIMT	Completed
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-N <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>NETWORK ACCESS &amp; AUTHENTICATION POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

Consistent standards for network access and authentication are critical to NWN Carousel information security and are often required by regulations or third-party agreements. Any user accessing NWN Carousel computer systems has the ability to affect the security of all users of the network. An appropriate Network Access and Authentication Policy reduces risk of a security incident by requiring consistent application of authentication and access standards across the network.

## 2.0 Scope

The scope of this policy includes all users who have access to company-owned or company-provided computers or require access to the corporate network and/or systems. This policy applies not only to employees, but also to guests, contractors, agents, and anyone requiring access to the corporate network. Public access to NWN Carousel externally reachable systems, such as its corporate website or public web applications, are specifically excluded from this policy.

## 3.0 Goals

The goals of this policy are to describe what steps must be taken to ensure that users connecting to the corporate network are authenticated in an appropriate manner, in compliance with company standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

## 4.0 Policy

### 4.1 Account Setup

During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

- Positive ID and coordination with Human Resources is required.
- Users will be granted least amount of network access required to perform his or her job function.
- Users will be granted access only if he or she accepts the Acceptable Use Policy.
- Access to the network will be granted in accordance with the Acceptable Use Policy.

### 4.2 Account Use

Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

- Accounts must be created using a standard format (i.e., firstname-lastname, or firstinitial-lastname, etc.)
- Accounts must be password protected (refer to the Password Policy for more detailed information).
- Accounts must be for individuals only. Account sharing and group accounts are not permitted.
- Identifiers cannot be re-used for at least two years, this includes individual accounts, groups, roles, services, or device identifiers.
- User accounts must not be given administrator or 'root' access unless this is necessary to perform his or her job function.
- Occasionally guests will have a legitimate business need for access to the corporate network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed.
- Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of CSOIT Management or executive team, or as required by applicable regulations or third-party agreements.

### 4.3 Multifactor Authentication

Based upon industry best practices and NIST Guidelines, NWN Carousel has implemented Multi-Factor Authentication for access to the Corporate network, O365 including email, and cloud systems that support MFA functionality. All employees must enroll a device for authentication purposes when configuring their MFA. Employees who do not wish to have their personal device enrolled or do not have a compatible device will be reviewed on a case-by-case basis by the Security Team.

#### **4.4 Account Termination**

When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee no longer works at NWN Carousel, that employee's account can be disabled. Human Resources must create a process to notify the CSOIT Team in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.).

#### **4.5 Account Suspension**

When an employee will be out of work for an extended period of time, NWN Carousel, for compliance and industry standard purposes, retains the right to temporarily disable access to corporate systems and resources for the duration of the absence. A request for account suspension will only be initiated by Human Resources in the form of a CSOIT Ticket for reasons including, but not limited to, extended leave such as short term disability, leave of absence, military leave, workers compensation, sabbatical, etc. Any employee meeting these criteria will have limited or no access to NWN Carousel resources for the duration of the absence. Identified resources include, but are not limited to the following systems and services:

- Corporate Network
- Corporate Systems and/or Applications
- Corporate Email
- Corporate Communications systems (ie: Skype, Desk Phone, Cell Phone)
- Facility Access

When an employee is scheduled to return to work, Human Resources will notify our internal support teams, via an internal support request, a minimum of two business days before the employee returns so as to afford necessary time to complete the re-enabling and testing of all user access and services. In the event a returning employee has access or systems support needs, all normal CSOIT procedures must be followed.

#### **4.6 Name Policy**

NWN Carousel recognizes that many of its employees use names other than their legal names to identify themselves. With this in mind, the company acknowledges that a "preferred name" can and should be used wherever possible except when required by a business or legal need, or when used for the purpose of misrepresentation.

Due to the sensitive nature of this type of change, all requests regarding name changes MUST go through the Human Resources Department. Upon receipt of a valid request, CSOIT will enter the preferred name into the Active Directory, which will display the preferred name in the company email, speech attendant and the PBX extension name.

#### **4.7 Authentication**

User machines must be configured to request authentication against the domain at startup. If the domain is not available or authentication for some reason cannot occur, then the machine should not be permitted to access the network.

#### **4.8 Use of Passwords**

When accessing the network locally, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to NWN Carousel Password Policy.

#### **4.9 Remote Network Access**

Remote access to the network can be provided for convenience to users but this comes at some risk to security. For that reason, NWN Carousel encourages additional scrutiny of users remotely accessing the network. NWN Carousel standards dictate that username and password is an acceptable means of authentication as long as appropriate policies are followed. Remote access must adhere to the Remote Access Policy.

#### **4.10 Screensaver Passwords**

Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason screensaver

passwords are required to be activated after 15 minutes of inactivity.

#### **4.11 Minimum Configuration for Access**

Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, users must strictly adhere to corporate standards with regard to antivirus software and patch levels on their machines. Users must not be permitted network access if these standards are not met. This policy will be enforced with product that provides network admission control.

#### **4.12 Encryption**

Industry best practices state that username and password combinations must never be sent as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication credentials must be encrypted during transmission across any network, whether the transmission occurs internal to NWN Carousel network or across a public network such as the Internet.

#### **4.13 Failed Logons**

Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password guessing and brute-force attempts, NWN Carousel must lock a user's account after 3 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the IT Manager.

#### **4.14 Non-Business Hours**

While some security can be gained by removing account access capabilities during non-business hours, NWN Carousel does not mandate time-of-day lockouts. This may be either to encourage working remotely, or because NWN Carousel business requires all-hours access.

#### **4.15 Administrator Accounts**

Companies must ensure IT administrators are provided and using separate and unique administrator accounts that are only used for administration responsibilities. Non-administration tasks must always be performed using non-administrator user accounts.

#### **4.16 Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

#### **4.17 Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

### **5.0 Revision History**


<b>Name</b>	<b>Date</b>	<b>Brief Description of Changes</b>	<b>Version</b>
James Aiello	7/15/11	Reformatted Policy	Version 1.1
James Aiello	10/28/11	Audited and added Name Policy	Version 1.2
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.0
James Aiello	3/4/16	Added language for Account Suspension	Version 2.1
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.2
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

### **6.0 Approval History**

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

**7.0 Review Cycle**

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	10/1/11	CIIMT	Completed
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-O <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>NETWORK SECURITY POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

NWN Carousel wishes to provide a secure network infrastructure in order to protect the integrity of corporate data and mitigate risk of a security incident. While security policies typically avoid providing overly technical guidelines, this policy is necessarily a more technical document than most.

## 2.0 Scope

This policy covers all of the Converged Support Groups systems and devices that comprise the corporate network or that are otherwise controlled by NWN Carousel.

## 3.0 Goals

The goal of this policy is to establish the technical guidelines for Information Technology security, and to communicate the controls necessary for a secure network infrastructure. The Network Security Policy will provide the practical mechanisms to support NWN Carousel comprehensive set of security policies. However, this policy purposely avoids being overly-specific in order to provide some latitude in implementation and management strategies.

## 4.0 Policy

### 4.1 Network Device Passwords

A compromised password on a network device could have devastating, network-wide consequences. Passwords that are used to secure these devices, such as routers, switches, and servers, must be held to higher standards than standard user-level or desktop system passwords. All Network Device Passwords must meet the “Administrator Password” requirements outlined in the NWN Carousel Password Policy along with the following additional standards:

- Passwords must be changed in accordance with the NWN Carousel Password Policy
- If any network device password is suspected to have been compromised, all network device passwords must be changed immediately.
- If a company network or system administrator leaves NWN Carousel, all passwords to which the administrator could have had access must be changed immediately. This statement also applies to any consultant or contractor who has access to administrative passwords.
- Vendor default passwords must be changed when new devices are put into service.

### 4.2 Logging

The logging of certain events is an important component of good network management practices. Logging needs vary depending on the type of network system, and the type of data the system holds. The following sections detail NWN Carousel requirements for logging and log review.

#### 4.2.a Application Servers

Logs from application servers are of interest since these servers often allow connections from a large number of internal and/or external sources. These devices are often integral to smooth business operations.

Examples: Web, email, database servers

Requirement: At a minimum, logging of errors, faults, and login failures is required. Additional logging is encouraged as deemed necessary. No passwords should be contained in logs.

#### 4.2.b Network Devices

Logs from network devices are of interest since these devices control all network traffic, and can have a huge impact on NWN Carousel security.

Examples: Firewalls, network switches, routers

Requirement: At a minimum, logging of errors, faults, and login failures is required. Additional logging is encouraged as deemed necessary. No passwords should be contained in logs.

#### 4.2.c Critical Devices

Critical devices are any systems that are critically important to business operations. These systems may



also fall under other categories above - in any cases where this occurs, this section shall supersede.  
Examples: File servers, lab or manufacturing machines, systems storing intellectual property  
Requirements: At a minimum, logging of errors, faults, and login failures is required. Additional logging is encouraged as deemed necessary. No passwords should be contained in logs.

#### **4.2.d Log Management**

While logging is important to NWN Carousel network security, log management can become burdensome if not implemented appropriately. As logs grow, so does the time required to review the logs. For this reason, NWN Carousel recommends that a log management application be considered.

#### **4.2.e Log Failures**

Systems will be configured to generate a support request and/or notify the NWN Carousel CSOIT team in the event of a failure with the Audit Logging process. Failures will be reviewed by the applicable engineering teams and worked as a Level 2 (High) support request.

#### **4.2.f Log Review**

Device logs do little good if they are not reviewed on a regular basis. Log management applications can assist in highlighting important events, however, a member of NWN Carousel CSOIT team should still review the logs as frequently as is reasonable.

#### **4.2.g Log Retention**

Logs should be retained in accordance with NWN Carousel Retention Policy. Unless otherwise determined by the CSOIT managers, logs should be considered operational data.

### **4.3 Firewalls**

Firewalls are arguably the most important component of a sound security strategy. Internet connections and other unsecured networks must be separated from NWN Carousel network through the use of a firewall.

#### **4.3.a Configuration**

The following statements apply to NWN Carousel implementation of firewall technology:

- Firewalls must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.
- No unnecessary services or applications should be enabled on firewalls. NWN Carousel should use 'hardened' systems for firewall platforms, or appliances.
- Clocks on firewalls should be synchronized with NWN Carousel other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.
- The firewall rule set must be documented and audited quarterly. Audits must cover each rule, what it is for, if it is still necessary, and if it can be improved.
- For its own protection, the firewall rule set must include a "stealth rule," which forbids connections to the firewall itself.
- The firewall must log dropped or rejected packets.

#### **4.3.b Outbound Traffic Filtering**

Firewalls are often configured to block only inbound connections from external sources; however, by filtering outbound connections from the network, security can be greatly improved. This practice is also referred to as "Egress Traffic Filtering."

Blocking outbound traffic prevents users from accessing unnecessary, and many times, dangerous services. By specifying exactly what outbound traffic to allow, all other outbound traffic is blocked. This type of filtering would block root kits, viruses, and other malicious tools if a host were to become compromised.

### **4.4 Networking Hardware**

Networking hardware, such as routers, switches, hubs, bridges, and access points, should be implemented in a consistent manner. The following statements apply to NWN Carousel implementation of networking hardware:

- Networking hardware must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.
- Clocks on all network hardware should be synchronized using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

- If possible for the application, switches are preferred over hubs. When using switches NWN Carousel should use VLANs to separate networks if it is reasonable and possible to do so.
- Access control lists must be implemented on network devices that prohibit direct connections to the devices. Connections to the router should be limited to the greatest extent possible. Exceptions to this are management connections that can be limited to known sources.
- Unused services and ports must be disabled on networking hardware.
- Access to administrative ports on networking hardware must be restricted to known management hosts and otherwise blocked with a firewall or access control list.

#### **4.5 Network Servers**

Servers typically accept connections from a number of sources, both internal and external. As a general rule, the more sources that connect to a system, the more risk that is associated with that system, so it is particularly important to secure network servers. The following statements apply to NWN Carousel use of network servers: Unnecessary files, services, and ports should be removed or blocked. If possible, follow a server-hardening guide, which is available from the leading operating system manufacturers.

Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.

If possible, a standard installation process should be developed for NWN Carousel network servers. This will provide consistency across servers no matter what employee or contractor handles the installation.

Clocks on network servers should be synchronized with NWN Carousel other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

#### **4.6 Collaborative Devices**

Collaborative devices present just as much risk to the environment as a server or an incorrectly configured device. Best standards will be used when connecting any collaborative computing device which includes remote meeting devices and applications, networked white boards, cameras, and microphones. Any and all devices that meet these parameters must be installed & configured in accordance with this manual by an IT staff member.

#### **4.7 Intrusion Detection/Intrusion Prevention**

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technology can be useful in network monitoring and security. The tools differ in that an IDS alerts to suspicious activity whereas an IPS blocks the activity. When tuned correctly, IDSs are useful but can generate a large amount of data that must be evaluated for the system to be of any use. IPSs automatically take action when they see suspicious events, which can be both good and bad, since legitimate network traffic can be blocked along with malicious traffic.

NWN Carousel requires the use of either an IDS or IPS on critical or high-risk network segments. If an IDS is used, procedures must be implemented to review and act on the alerts expeditiously. If an IPS is used, procedures must be implemented that provide a mechanism for emergency unblocking if the IPS obstructs legitimate traffic. Also, if an IPS is used, it should be audited and documented according to the standards detailed in the "Firewalls" section of this document.

#### **4.8 Security Testing**

Security testing, also known as a vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining NWN Carousel network security. Security testing can be provided by IT Staff members, but is often more effective when performed by a third party with no connection to NWN Carousel day-to-day Information Technology activities. The following sections detail NWN Carousel requirements for security testing.

##### **4.8.a Internal Security Testing**

Internal security testing does not necessarily refer to testing of the internal network, but rather testing performed by members of NWN Carousel CSOIT team. Internal testing should not replace external testing; however, when external testing is not practical for any reason, or as a supplement to external testing, internal testing can be helpful in assessing the security of the network.

Internal security testing is allowable, but only by employees whose job functions are to assess security, and only with permission of the CSOIT Managers. Internal testing should have no measurable negative impact on NWN Carousel systems or network performance.

##### **4.8.b External Security Testing**

External security testing, which is testing by a third party entity, is an excellent way to audit NWN Carousel security controls. The CSOIT Manager must determine to what extent this testing should be performed, and what systems/applications it should cover.

External testing must not negatively affect network performance during business hours or network security at any time.

As a rule, "penetration testing," which is the active exploitation of company vulnerabilities, should be

discouraged. If penetration testing is performed, it must not negatively impact company systems or data. NWN Carousel encourages external security testing, but does not provide rigid guidelines regarding at what intervals the testing should occur. Testing should be performed as often as is necessary, as determined by the CSOIT Management.

#### **4.9 Audit Security**

This policy details the standards that must be implemented for security monitoring and audit control. It includes specifications for audit trails and monitoring.

- Audit logs will be maintained to provide accountability for user actions on the NWN network.
- The following actions on the network will be recorded:
  - Successful Logon and Logoff Events
  - Failed Logon Events
  - System Events (e.g. Startup, Shutdown and Process Tracking)
- The following actions on the network will be monitored:
  - Failed Logon Events
  - System Events (e.g. Startup, Shutdown, Faults and Process Tracking)
- For each audit log entry, the following information will be recorded:
  - Date and Time of Events
  - User ID of User Involved in an Event
  - Type of User Action
- Audit logs will not be modified.
- Only security administrators will be able to view the audit logs.
- The CSOIT Team will ensure that security-related incidents are logged and that the logs are reviewed immediately.
- Whenever possible, audit logs will be sized properly to support the companies log backup and review process.
- Audit logs will be configured not to overwrite within the log backup period.
- Audit logs will be configured to capture all target transaction within the log backup period.
- Audit logs will be configured to a consistent size for all systems.

#### **4.10 Disposal of Information Technology Assets**

CSOIT assets, such as network servers and routers, often contain sensitive data about NWN Carousel network communications. When such assets are decommissioned, the following guidelines must be followed:

- Any asset tags or stickers that identify NWN Carousel must be removed before disposal.
- Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.
- Physical destruction of the device's data storage mechanism (such as its hard drive or solid state memory) is required. If physical destruction is not possible, the CSOIT Management must be notified.

#### **4.11 Network Compartmentalization**

Good network design is integral to network security. By implementing network compartmentalization, which is separating the network into different segments, NWN Carousel will reduce its network-wide risk from an attack or virus outbreak. Further, security can be increased if traffic must traverse additional enforcement/inspection points. NWN Carousel requires the following with regard to network compartmentalization:

##### **4.11.a Higher Risk Networks**

Examples: Guest network, wireless network

Requirements: Segmentation of higher risk networks from NWN Carousel internal network is required, and must be enforced with a firewall or router that provides access controls.

##### **4.11.b Externally-Accessible Systems**

Examples: Core, Management, Server, Backbone, Voice

Requirements: Segmentation of internal networks from one another can improve security as well as reduce chances that a user will access data that he or she has no right to access. NWN Carousel requires that networks be segmented to the fullest reasonable extent.

##### **4.11.c Internal Networks**

Examples: Core, Management, Server, Backbone, Voice

Requirements: Segmentation of internal networks from one another can improve security as well as

reduce chances that a user will access data that he or she has no right to access. NWN Carousel requires that networks be segmented to the fullest reasonable extent.

#### **4.12 Network Documentation**

Network documentation, specifically as it relates to security, is important for efficient and successful network management. Further, the process of regularly documenting the network ensures that NWN Carousel CSOIT Team has a firm understanding of the network architecture at any given time. The intangible benefits of this are immeasurable.

At a minimum, network documentation must include:

- Network diagram(s)
- System configurations
- Firewall rule set
- IP Addresses
- Access Control Lists

NWN Carousel requires that network documentation be performed and updated on a yearly basis.

#### **4.13 Antivirus/Anti-Malware**

Computer viruses and malware are pressing concerns in today's threat landscape. If a machine or network is not properly protected, a virus outbreak can have devastating effects on the machine, the network, and the entire company. NWN Carousel provides the following guidelines on the use of antivirus/anti-malware software:

- All company-provided user workstations must have antivirus/anti-malware software installed.
- Workstation software must maintain a current "subscription" to receive patches and virus signature/definition file updates.
- Patches, updates, and antivirus signature file updates must be installed in a timely manner, either automatically or manually
- In addition to the workstation requirements, virus and malware scanning must be implemented at the Internet gateway to protect the entire network from inbound threats.

#### **4.14 Software Use Policy**

Software applications can create risk in a number of ways, and thus certain aspects of software use must be covered by this policy. NWN Carousel provides the following requirements for the use of software applications:

- Only legally licensed software may be used. Licenses for NWN Carousel software must be stored in a secure location.
- Open source and/or public domain software can only be used with the permission of the CSOIT Team.
- Software should be kept reasonably up-to-date by installing new patches and releases from the manufacturer.
- Vulnerability alerts should be monitored for all software products that NWN Carousel uses. Any patches that fix vulnerabilities or security holes must be installed expediently.

#### **4.15 Maintenance Windows and Scheduled Downtime**

Certain tasks require that network devices be taken offline, either for a simple re-boot, an upgrade, or other maintenance. When this occurs, the CSOIT Team must perform the tasks before and after normal business hours. Tasks that are deemed "emergency support," as determined by the CSOIT Management, can be performed at any time.

#### **4.16 Change Management**

Documenting changes to network devices is a good management practice and can help speed resolution in the event of an incident. The CSOIT Team must document hardware and/or configuration changes to network devices in a "change log."

#### **4.17 Suspected Security Incidents**

When a security incident is suspected that may impact a network device, the CSOIT Team will refer to NWN Carousel Incident Response policy for guidance.

#### **4.18 Redundancy**

Redundancy can be implemented on many levels, from redundancy of individual components to full site-redundancy. As a general rule, the more redundancy implemented, the higher the availability of the device or network, and the higher the associated cost. NWN Carousel wishes to provide the CSOIT Managers with latitude to determine the appropriate level of redundancy for critical systems and network devices. Redundancy should be implemented where it is needed, and should include some or all of the following:

- Hard drive redundancy, such as mirroring or RAID
- Server level redundancy, such as clustering or high availability

- Component level redundancy, such as redundant chassis, power supplies or redundant NICs
- Keeping hot or cold spares onsite

#### **4.19 Manufacturer Support Contracts**

Outdated products can result in a serious security breach. When purchasing critical hardware or software, NWN Carousel must purchase a maintenance plan, support agreement, or software subscription that will allow NWN Carousel to receive updates to the software and/or firmware for a specified period of time. The plan must meet the following minimum requirements:

- Hardware: The arrangement must allow for repair/replacement of the device within an acceptable time period, as determined by the CSOIT Management, as well as firmware or embedded software updates.
- Software: The arrangement must allow for updates, upgrades, and hotfixes for a specified period of time.

#### **4.20 Security Policy Compliance**

It is NWN Carousel intention to comply with this policy not just on paper but in its everyday processes as well. With that goal in mind NWN Carousel requires the following:

##### **4.20.a Security Program Ownership**

The Director of Security Risk & Compliance is responsible for NWN Carousel compliance with this security policy and any applicable security regulations. This employee is responsible for:

1. The initial implementation of the security policies,
2. Ensuring that the policies are disseminated to employees,
3. Training and retraining of employees on NWN Carousel information security program (as detailed below),
4. Any ongoing testing or analysis of NWN Carousel security in compliance with this policy,
5. Updating the policy as needed to adhere with applicable regulations and the changing information security landscape.

##### **4.20.b Security Training**

Improperly trained or uninformed users and system administrators are a major threat to system security. The best system administrator cannot enforce security alone and must rely on users taking responsibility for system security. This policy strives to ensure new system administrators and users complete internal training programs, understand NWN security practices, recognize security problems and understand what to do if security problems occur.

A training program has been implemented that will detail NWN Carousel information security program to all users and/or employees covered by the policy, as well as the importance of data security.

Employees must sign off on the receipt of, and in agreement to, the user-oriented policies. Re-training should be performed at least annually. Additionally, the policies should be reviewed when there is an information security incident or a material change to NWN Carousel security policies. The following details will apply to all NWN Carousel employees:

- All personnel will read and sign the NWN Security Policy before obtaining system access to any corporate computing assets.
- All new users must attend an approved security awareness training class prior to, or at least within 30 days of, being granted access to any system. The security awareness training class includes, but is not limited to Phishing, Security Awareness, HIPAA for Business Associates and Global Privacy and Data Protection (GDPR).
- All personnel with access to corporate computing assets will receive annual refresher security training.
- Each user is trained on how to identify and report common security incidents.
- Security policies, procedures, and manuals are readily available for reference and review by the appropriate staff/user.
- All personnel will be instructed to report any potential security weaknesses immediately to a member of the CSOIT Team.

##### **4.20.c Security Policy Review**

NWN Carousel security policies should be reviewed at least annually. Additionally, the policies should be reviewed when there is an information security incident or a material change to NWN Carousel security policies. As part of this evaluation NWN Carousel should review:

- Any applicable regulations for changes that would affect NWN Carousel compliance or the effectiveness of any deployed security controls.

- If NWN Carousel deployed security controls are still capable of performing their intended functions.
- If technology or other changes may have an effect on NWN Carousel security strategy.
- If any changes need to be made to accommodate future IT security needs.

#### 4.21 **Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

#### 4.22 **Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

### 5.0 **Revision History**


Name	Date	Brief Description of Changes	Version
James Aiello	8/26/11	Reformatted Network Security Policy	Version 1.1
James Aiello	10/31/11	Reformatted Network Security Policy	Version 1.2
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.0
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.1
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

### 6.0 **Approval History**

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

### 7.0 **Review Cycle**

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-P <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>PASSWORD POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

A solid Password Policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

## 2.0 Scope

This policy applies to any person who is provided an account on the organization's network or systems, including: employees, guests, contractors, partners, vendors, etc.

## 3.0 Goals

The goal of this policy is to specify guidelines for use of passwords. Most importantly, this policy will help users understand why strong passwords are a necessity, and help them create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

## 4.0 Policy

### 4.1 Requirements

- The best security against a password incident is simple: following a sound password construction strategy. The organization mandates that users adhere to the following guidelines on password construction:
- User Passwords must be at least 12 characters
- Administrative Account passwords must be 16 characters
- Passwords must be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)
- Passwords must be comprised of a mix of upper and lower case characters
- Passwords must not be comprised of, or otherwise utilize, words that can be found in a dictionary
- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
- Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.
- Users may reuse passwords only after 10 different passwords have been used.
- After changing their password, users must wait at least 24 hours before they will be allowed to change it again. Password expiration warnings will be provided fourteen days prior to the password expiration.

### 4.2 Confidentiality

- Passwords should be considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of organization passwords:
- Users must not disclose their passwords to anyone
- Users must not share their passwords with others (co-workers, supervisors, family, etc.)
- Users must not write down their passwords and leave them unsecured Users must not check the "save password" box when authenticating to applications
- Users must not use the same password for different systems and/or accounts
- Users must not send passwords via email
- Users must not re-use passwords

#### 4.2.a Support

- During the process of support and troubleshooting, CSOIT team members can and may reset an employee's password to resolve an issue that the end user is experiencing. Once the issue has been resolved the employee must reset their network password.
- Due to the level of trust placed on the CSOIT team by the NWN Carousel executives it is acceptable for an employee to provide a CSOIT member with their network password via telephone only to aid in the troubleshooting process. Once the issue has been resolved the employee must reset their network password.
- CSOIT must verify identity of individual before resetting password

- Custodians will enforce required password changes out of cycle for certain security events that have the potential for security compromises (e.g., employee relocation, intrusion attempt, or employee termination).

### 4.3 **Change Frequency**

In order to maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. At a minimum, users must change passwords every 180 days. The organization may use software that enforces this policy by expiring users' passwords after this time period.

### 4.4 **Multifactor Authentication**

Based upon industry best practices and NIST Guidelines, NWN Carousel has implemented Multi-Factor Authentication for access to the Corporate network, O365 including email, and cloud systems that support MFA functionality. All employees must enroll a device for authentication purposes when configuring their MFA. Employees who do not wish to have their personal device enrolled or do not have a compatible device will be reviewed on a case-by-case basis by the Security Team.

### 4.5 **Incident Reporting**

Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the CSOIT Managers. Any request for passwords over the phone or email, whether the request came from organization personnel or not, should be expediently reported. When a password is suspected to have been compromised CSOIT will request that the user, or users, change all his or her passwords. Passwords will be changed as soon as possible, but no more than 24 hours of a possible compromise. Every effort will be made to disable these accounts as soon as possible. Corporate servers will be configured not to retain account or password information from previous logins.

### 4.6 **Administrator Accounts**

As a general rule, administrative (also known as "root") access to systems should be limited to only those who have a legitimate business need for this type of access. This is particularly important for network devices, since administrative changes can have a major effect on the network, and, as such, network security. Additionally, administrative access to network devices should be logged.

Management must ensure Information Technology administrators are provided and using separate and unique administrator accounts that are only used for administration responsibilities. Non-administration tasks must always be performed using the users personal account. In order to ensure these sensitive accounts are kept secure, minimum password length for administrative accounts is 16 characters.

### 4.7 **Failed Logons**

Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password guessing and brute-force attempts, NWN Carousel must lock a user's account after 5 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the CSOIT Managers.

In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

### 4.8 **Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

### 4.9 **Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

## 5.0 **Revision History**

Name	Date	Brief Description of Changes	Version
------	------	------------------------------	---------




James Aiello	7/25/11	Reformatted Password Policy	Version 1.1
James Aiello	10/31/11	Reformatted Password Policy	Version 1.2
James Aiello	10/6/14	Edited Password Policy per CIIMT Audit	Version 2.0
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.1
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.2
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

## 6.0 Approval History

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

## 7.0 Review Cycle

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	10/1/14	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-Q <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>PATCH MANAGEMENT POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

Throughout the lifecycle of a product, firmware patches and upgrades are released to provide both feature and security updates. While some patches and upgrades are necessary, they may cause issues including outages and the degradation of the end user experience. The following processes and procedures are in place to balance security and stability for NWN Carousel workstations, systems, and infrastructure.

## 2.0 Scope

This policy applies to all critical and/or security patches for hardware and software owned or managed by NWN Carousel. Note that feature patches or updates that are not security related do not fall within the parameters of this policy.

## 3.0 Goals

To address technical systems and software vulnerabilities quickly and effectively in order to reduce the likelihood of vulnerabilities being exploited and serious business impact arising.

## 4.0 Patch Management

All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. System components and devices attached to the NWN Carousel network must be regularly maintained including the application of critical security patches within 30 days after release by the vendor and moderate vulnerabilities within 90 days. Other patches not designated as critical by the vendor must be applied on a normal maintenance schedule, which may depart from the above. Note: Critical security patches will be identified according to a risk ranking process.

### 4.1 Patch Identification

In order to identify required patches and updates, CSOIT will monitor releases through various sources including, but not limited to, Microsoft TechNet, US-CERT, Symantec, SANS, applicable vendors, and NWN Carousel’s patch management tool.

### 4.2 Patch Testing

Due to the various integrations and dependencies within the Carousel network, all patches will be tested prior to implementing in production. Testing will preferably be performed within the Lab environment when possible. Once validated, patches will first be tested on a small subset of the organization prior to a widespread deployment.

### 4.3 Patch Deployment

In order to meet industry standards, critical patches for identified vulnerabilities will be applied within 30 days of release where possible. For select business systems identified as “service critical” updates and patches will be deployed on a quarterly basis to ensure a minimal impact to service delivery and by extent, our customers. In the event that NWN Carousel is unable to deploy a specific patch due to faults found during testing, the Security team will be notified so that the correct documentation can be notated.

Patches on production systems (e.g. servers) may require complex testing and installation procedures. In certain cases, risk mitigation, rather than patching, may be preferable. The risk mitigation alternative selected should be in proportion to the risk. The reason for any departure from the above standard and alternative protection measures taken must be documented in writing for devices storing non-public data.

### 4.4 Vulnerability Scanning

In order to ensure the integrity of NWN Carousel’s Corporate Network, vulnerability scanning will be performed on a monthly basis. All items identified as a Critical or High vulnerability will be remediated within the 30 day window prescribed above.

#### 4.5 System End of Life/End of Support

At some point, most systems will reach a point where they are no longer supported by their manufacture. This poses a problem from a vulnerability perspective as patches will not be available from a performance and/or security perspective. As such, NWN Carousel will analyze its tools as they approach EOL/EOS to determine the best path forward. In most cases, the replacement of said systems will be necessary. In the event of a core critical system that cannot be replaced, risk mitigation strategies must be put into place which may include:

- The engagement of a third party to support the tool
- Segregation/removal of system from corporate network
- Enhanced access mechanisms
- Further limitation of access

#### 4.6 Integrity Verification Tools

Where able, NWN Carousel will ensure manufactures have integrity verification enabled for software & patches that may house sensitive information. This allows the detection of unauthorized changes to software and firmware components using developer-provided tools, techniques, and mechanisms.

#### 4.7 Applicability of Other Policies

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

#### 4.8 Enforcement

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

### 5.0 Revision History


Name	Date	Brief Description of Changes	Version
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

### 6.0 Approval History

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

### 7.0 Review Cycle

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-R <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>PHYSICAL SECURITY POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

Information assets are necessarily associated with the physical devices on which they reside. Information is stored on workstations and servers and transmitted on NWN Carousel physical network infrastructure. In order to secure NWN Carousel data, thought must be given to the security of NWN Carousel physical Information & Technology (IT) resources to ensure that they are protected from standard risks.

## 2.0 Scope

This policy applies to the physical security of NWN Carousel information systems, including, but not limited to, all company-owned or company-provided network devices, servers, personal computers, mobile devices, and storage media. Additionally, any person working in or visiting NWN Carousel office is covered by this policy.

Please note that this policy covers the physical security of NWN Carousel Information & Technology infrastructure, and does not cover the security of non-IT items or the important topic of employee security. While there will always be overlap, care must be taken to ensure that this policy is consistent with any existing physical security policies.

## 3.0 Goals

The goal of this Physical Security Policy is to protect NWN Carousel physical information systems by setting standards for secure operations.

## 4.0 Policy

### 4.1 Choosing a Site

When possible, thought should be given to selecting a site for IT Operations that is secure and free of unnecessary environmental challenges. This is especially true when selecting a datacenter or a site for centralized IT operations. At a minimum, NWN Carousel site should meet the following criteria:

- A site should not be particularly susceptible to fire, flood, earthquake, or other natural disasters.
- A site should not be located in an area where the crime rate and/or risk of theft is higher than average.
- A site should have the fewest number of entry points possible.

### 4.2 Security Zones

At a minimum, NWN Carousel will maintain standard security controls, such as locks on exterior doors and/or an alarm system, to secure NWN Carousel assets. In addition to this NWN Carousel must provide security in layers by designating different security zones within the building. Security zones should include:

#### 4.2.a Public

This includes areas of the building or office that are intended for public access.

- Access Restrictions: NO Public Areas
- Additional Security Controls: None
- Examples: Lobby, common areas of building

#### 4.2.b Company

This includes areas of the building or office that are used only by employees and other persons for official company business.

- Access Restrictions: Only company personnel and approved/escorted guests
- Additional Security Controls: Additional access controls should be used, such as keys, keypads, keycards, or similar devices, with access to these areas logged if possible.
- Examples: Hallways, private offices, work areas, conference rooms

#### 4.2.c Private

This includes areas that are restricted to use by certain persons within NWN Carousel, such as executives, engineers, and IT personnel, for security or safety reasons.

- Access Restrictions: Only specifically approved personnel

- Additional Security Controls: Additional access controls must be used, such as keys, keypads, keycards, or similar devices, with access to these areas logged. Additionally, an alarm system should be considered for these areas that will alert to unauthorized access.
- Examples: Executive offices, lab space, network room, HR, financial offices, and storage areas.

### 4.3 **Access Controls**

Access controls are necessary to restrict entry to NWN Carousel premises and security zones to only approved persons. There are a several standard ways to do this, which are outlined in this section, along with NWN Carousel guidelines for their use.

#### 4.3.a **Keys & Keypads**

The use of keys is prohibited as a security mechanism. Keypads may be used in non-private areas. These security mechanisms are the most inexpensive and are the most familiar to users. The disadvantage is that NWN Carousel has no control, aside from changing the locks or codes, over how and when the access is used. Keys can be copied and keypad codes can be shared or seen during input.

#### 4.3.b **Keycards & Biometrics**

NWN Carousel requires that keycards or biometrics be used for all user access controls. NWN Carousel must use this technology to enforce security zones and provide employees the least amount of access required to do their jobs.

Keycards and biometrics have an advantage over keys in that access policies can be tuned to the individual user. Schedules can be set to forbid off-hours access, or forbid users from accessing a security zone where they are not authorized. Perhaps best of all, these methods allow for control over exactly who possesses the credentials. If a keycard is lost or stolen it can be immediately disabled. If an employee is terminated or resigns, that user's access can be disabled. The granular control offered by keycards and biometrics makes them appealing access control methods.

#### 4.3.c **Alarm System**

A security alarm system is a good way to minimize risk of theft, or reduce loss in the event of a theft and will be used for offices that are not staffed on 24X7 basis.

### 4.4 **Physical Data Security**

Certain physical precautions must be taken to ensure the integrity of NWN Carousel data. At a minimum, the following guidelines must be followed:

- Computer screens must be positioned where information on the screens cannot be seen by outsiders.
- Confidential and sensitive information must not be displayed on a computer screen where the screen can be viewed by those not authorized to view the information.
- Users must log off, lock or shut down their workstations when leaving for an extended time period, or at the end of the workday.
- Network cabling must not run through non-secured areas unless the cabling is carrying only public data (i.e., extended wiring for an Internet circuit).
- Network ports that are not in use must be disabled.

### 4.5 **Physical System Security**

In addition to protecting the data on NWN Carousel information technology assets, this policy provides the guidelines below on keeping the systems themselves secure from damage or theft.

#### 4.5.a **Minimizing Risk of Loss and Theft**

In order to minimize the risk of data loss through loss or theft of company property, the following guidelines must be followed:

- Unused systems: If a system is not in use for an extended period of time it should be moved to a secure area or otherwise secured.
- Mobile devices: Special precautions must be taken to prevent loss or theft of mobile devices. Refer to NWN Carousel Mobile Device Policy for guidance.
- Systems that store confidential data: Special precautions must be taken to prevent loss or theft of these systems. Refer to NWN Carousel Confidential Data Policy for guidance.

#### 4.5.b **Minimizing Risk of Damage**

Systems that store company data are often sensitive electronic devices that are susceptible to being inadvertently damaged. In order to minimize the risk of damage, the following guidelines must be followed:

- Environmental controls should keep the operating environment of company systems within standards specified by the manufacturer. These standards often involve, but are not limited to, temperature and humidity.
- Proper grounding procedures must be followed when opening system cases. This may include use of a grounding wrist strap or other means to ensure that the danger from static electricity is minimized.
- Strong magnets must not be used in proximity to company systems or media.
- Except in the case of a fire suppression system, open liquids must not be located above company systems. Technicians working on or near company systems should never use the systems as tables for beverages. Beverages must never be placed where they can be spilled onto company systems.
- Uninterruptible Power Supplies (UPSs) and/or surge-protectors are required for important systems and encouraged for all systems. These devices must carry a warranty that covers the value of the systems if the systems were to be damaged by a power surge.

#### **4.6 Electrical Considerations**

Electricity is a special threat for computer systems. Computer equipment is highly sensitive to any disruption of electrical service and to the quality of service supplied. If there are peaks or surges in the service, information can be lost and equipment may be damaged. This policy discusses necessary provisions that will prevent such occurrences and procedures that should be followed if electrical service is interrupted.

- Critical systems will be isolated and conditioned power supplies will be used to provide electrical power to those systems.
- Uninterruptible Power Systems (UPS) are required to support network servers and other mission critical systems.
- Backup power systems will be tested monthly and evaluated to ensure proper operation of systems and procedures.
- All electro-mechanical door locks and fire alarm systems must be connected to an Uninterruptible Power System (UPS).
- Emergency power-offs will be protected from accidental activation.
- All electrical circuit breakers will conform to commercial building codes.
- All electrical and communication cabling should be physically secured into and out of all facilities.

#### **4.7 Fire Prevention**

It is NWN Carousel policy to provide a safe workplace that minimizes the risk of fire. In addition to the danger to employees, even a small fire can be catastrophic to computer systems. Further, due to the electrical components of IT systems, the fire danger in these areas is typically higher than other areas of NWN Carousel office. The guidelines below are intended to be specific to NWN Carousel information technology assets and should conform to NWN Carousel overall fire safety policy.

- Fire, smoke alarms, and/or suppression systems must be used, and must conform to local fire codes and applicable ordinances.
- Electrical outlets must not be overloaded. Users must not chain multiple power strips, extension cords, or surge protectors together.
- Extension cords, surge protectors, power strips, and uninterruptible power supplies must be of the three-wire/three-prong variety.
- Only electrical equipment that has been approved by Underwriters Laboratories and bears the UL seal of approval must be used.
- Unused electrical equipment should be turned off when not in use for extended periods of time (i.e., during non-business hours) if possible.
- Periodic inspection of electrical equipment must be performed. Power cords, cabling, and other electrical devices must be checked for excessive wear or cracks. If overly worn equipment is found, the equipment must be replaced or taken out of service immediately depending on the degree of wear.
- A smoke alarm monitoring service must be used that will alert a designated company employee if an alarm is tripped during non-business hours.

#### **4.8 Entry Security**

It is NWN Carousel policy to provide a safe workplace for employees. Monitoring those who enter and exit the premises is a good security practice in general, but is particularly true for minimizing risk to company systems and data. The guidelines below are intended to be specific to NWN Carousel information technology assets and should conform to NWN Carousel overall security policy.

##### **4.8.a Use of Identification Badges**

Identification (ID) badges are useful to identify authorized persons on NWN Carousel premises. NWN

Carousel has established the following guidelines for the use of ID badges.

- Employees: ID badges are required and must be displayed at all times while on company premises. Employees should remove their badges from view when out of the office.
- Non-employees/Visitors: Visitor badges are required. If possible, specific, non-generic, badges should identify visitors by name.
- Users must report a lost or stolen badge immediately to his or her supervisor and the internal IT team. A temporary badge may be utilized in such cases until a badge can be re-generated.
- Initial badge generation will be done only at the direction of Human Resources for new hires or users changing jobs. Users must show photo identification for identity verification.

#### **4.8.b Sign-in Requirements**

NWN Carousel must maintain a sign-in log (or similar device) in the lobby or entry area and visitors must be required to sign in upon arrival. At minimum, the register must include the following information: visitor's name, company name, reason for visit, name of person visiting, sign-in time, and sign-out time.

#### **4.8.c Visitor Access**

Visitors should be given only the level of access to NWN Carousel premises that is appropriate to the reason for their visit. After checking in, visitors must be escorted unless they are considered "trusted" by NWN Carousel. Examples of a trusted visitor may be NWN Carousel legal counsel, vendor representative, financial advisor, or a courier that frequents the office, and will be decided on a case-by-case basis.

### **4.9 Removal of Equipment from Data Centers**

The following controls are in place to prevent the removal of maintenance equipment containing organizational information:

- a. Engineer must verify that there is no organizational information contained on the equipment;
- b. Sanitizing or destroying the equipment by approved vendors
- c. Retaining the equipment within the facility; or
- d. Obtaining an exemption from the NWNC Security Team explicitly authorizing removal of the equipment from the facility.

### **4.10 Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

### **4.11 Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

## **5.0 Revision History**

<b>Name</b>	<b>Date</b>	<b>Brief Description of Changes</b>	<b>Version</b>
James Aiello	7/15/11	Reformatted Outsourcing Policy	Version 1.1
James Aiello	10/31/11	Reformatted Outsourcing Policy	Version 1.2
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.0
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.1
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.2
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.3
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1


## 6.0 Approval History

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methe	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

## 7.0 Review Cycle

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	6/1/12	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	10/10/21	SRC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled



	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-S <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>PRIVACY POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

This document is not intended as a customer-facing document, but as an internal document for NWN Carousel employees to reference for the company policy on information privacy.

## 2.0 Scope

All policies and procedures are expected to conform to the standards set by this document. This is necessary to ensure the continuity of policy documentation within the Information Security Manual.

## 3.0 Goals

The goal of this policy is to provide the business with documented standards for our approach to handling the various types of information employees may come into contact with.

## 4.0 Policy

### 4.1 Information Security Standards

There are many different levels of standards when discussing Information Security based upon the classification of the information in question. In this section, we will examine the primary types of information covered under a privacy policy, specifically, Personally Identifiable Information (PII) and Personal Health Information (PHI).

#### 4.1.a Personally Identifiable Information (PII)

For the purpose of this policy, Personally Identifiable Information (PII) is defined as information that can be used to identify an individual, including, but not limited to: name, address, date of birth, marital status, contact information, ID issue and expiry date, and intentions to acquire goods and services. If an individual chooses to provide NWN Carousel with personal information, the personal information will be used solely by and transferred only to NWN Carousel, its offices and subsidiaries around the world, its resellers and distributors and service providers, which are those companies contracted by NWN Carousel to deliver requested information and services. We may also transfer personal information across borders and from the individual's country or jurisdictions to NWN Carousel' offices and subsidiaries, its resellers and distributors and service providers around the world. An individual's personal information is typically not shared outside NWN Carousel without permission, except under conditions explained below. NWN Carousel may send personal information to other service provider companies under any of the following circumstances:

- When we have an individual's consent to share the information
- If sharing an individual's information is necessary to provide a product or service that is requested (If personal information is shared with third parties we will only provide the information they need to deliver the service. Also, such companies are prohibited from using such personal information for any other purpose)
- As part of a joint sales promotion or to pass sales leads to one of our distribution partners; and
- To keep an individual up to date on the latest product announcements, product updates, special offers or other information we think he/she would like to hear about either from us or from our service providers (unless the individual has opted out of these types of communications).

We will also disclose personal information if required or permitted to do so by law, or in urgent circumstances, to protect personal safety, the public or our websites.

#### 4.1.a.a. Notice and Ability to Opt-Out

When PII is collected, NWN Carousel will typically inform the individual at the point of collection or upon our first communication to the individual the purpose for the collection and where appropriate, allow the individual to elect whether to provide the information to NWN Carousel and/or specify how we can use such personal information.

NWN Carousel provides individuals who elect to receive electronic or other communications the ability to "opt-out" of those communications by sending us a notice to unsubscribe. NWN Carousel respects your wishes and will discontinue communicating with individuals who have requested not to receive email or other communications from NWN Carousel. This

means we assume an individual has given us consent to collect and use his/her personal information in accordance with this Policy unless the individual has taken affirmative action to indicate that he/she does not consent, for instance by clicking or checking the appropriate option or box at the point of collection. In some cases, when applicable, NWN Carousel will provide an individual with the opportunity to "opt-in." This means that we will require affirmative action from the individual to indicate his/her consent before we use personal information for purposes other than the purpose for which the personal information was submitted.

#### **4.1.a.b. Safeguards**

NWN Carousel safeguards the security of the personal information and other data provided to us with physical, electronic and managerial procedures. Inside NWN Carousel, data is stored in secure and controlled servers with limited access. Your information may be stored and processed in the United States or any other country where NWN Carousel, its subsidiaries or service providers are located.

#### **4.1.b Protected Health Information (PHI)**

During the normal course of business process, NWN Carousel does not transmit or process any of the information, which meets the definition of "Protected Health Information" or PHI. PHI is defined as information in any form that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care of an individual; or the past, present, or future payment for the provision of health care to an individual. In rare circumstances, a NWN Carousel employee may come into contact with some form of Protected Health Information during while providing a service to our customers. In these cases, Carousel is committed to ensuring our customer meet their requirements under HIPPA and HITECH and as such, has the following policies in place.

##### **4.1.b.a. Reporting Data Breach**

The term "Breach" means the acquisition, access, use, or disclosure of "Protected Health Information" by a covered entity and includes information in both physical and electronic form.

Carousel shall report to the customer in writing of any Breach of Protected Health Information that it becomes aware within 48 hours of discovery. Written notice shall contain:

- The date of discovery of the Breach;
- A listing of the identification of individuals and/or classes of individuals who are subject to the Breach
- A general description of the nature of the Breach.

It is the sole responsibility of the customer to notify its patients of any breach of Protected Health Information. At no time, will NWN Carousel contact or speak directly to any customers patients/individuals who are the subject of any Breach. NWN Carousel shall cooperate with customers to assist in notification and any details pertaining to any Breach of Protected Health Information.

##### **4.1.b.b. Use of PHI**

NWN Carousel may use Protected Health Information to report violations of the law to appropriate Federal and State authorities, consistent with 164.502(j)(1).

##### **4.1.b.c. Business Associate Agreements**

If & when applicable, NWN Carousel sub-contractors will enter into a binding Business Associate Agreement if services to be rendered are for a client which NWN Carousel has a signed Business Associate Agreement.

#### **4.2 Information Security Awareness Program**

In order to meet compliance requirements for certain customers, all NWN Carousel employees are required to participate in an annual Information Security Awareness Program. This program will address basic information security requirements such as secure password formation and physical security measures to ensure that information remains secure. In addition, this program will provide staff with the businesses expectations in regards to PII & PHI, and the required process if an employee becomes aware of a data breach.

#### **4.3 Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in

disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

## 5.0 Revision History


Name	Date	Brief Description of Changes	Version
James Aiello	11/28/12	Created Draft of Privacy Policy	Version 0.1
James Aiello	11/23/12	Finalized Privacy Policy	Version 1.0
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.0
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.1
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

## 6.0 Approval History

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

## 7.0 Review Cycle

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	10/10/21	SRC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-T <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>REMOTE ACCESS POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

This policy is provided to define standards for accessing corporate information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium.

## 2.0 Scope

The scope of this policy covers all employees, contractors, and external parties that access company resources over a third-party network. This policy only specifically excludes non-company provided equipment from accessing the network.

## 3.0 Goals

It is often necessary to provide access to corporate information resources to employees or others working outside the NWN Carousel network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation.

## 4.0 Policy

### 4.1 Prohibited Actions

Remote access to corporate systems is only to be offered through a company provided means of remote access in a secure fashion. The following are specifically prohibited:

- Installing a modem, router, or other remote access device on a company system without the approval of CSOIT.
- Remotely accessing corporate systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC without documented approval from CSOIT.
- Use of non-company-provided remote access software.
- Split Tunneling to connect to an insecure network in addition to the corporate network, or in order to bypass security restrictions.

### 4.2 Non-Company Provided Machines

Accessing the corporate network through home or public machines presents a serious security risk, as NWN Carousel cannot ensure the security of the device accessing the network. It is with this reasoning that NWN Carousel explicitly prohibits any non-company provided machines access the network. For the purpose of this policy, expensed mobile devices are allowed on the network provided they meet all the requirements set forth in the Network Access Policy. Exceptions can be made on a case by case basis for Vendors that have undergone a thorough Security Audit to ensure they meet current NWN Carousel Security Standards.

### 4.3 Client Software

NWN Carousel will supply users with remote access software that allows for secure access and enforces the remote access policy. The software will provide traffic encryption in order to protect the data during transmission as well as a firewall that protects the machine from unauthorized access.

### 4.4 Network Access

NWN Carousel will limit all remote users' access privileges to only those information assets that are reasonable and necessary to perform his or her job function when working remotely (i.e., email). The entire network must not be exposed to remote access connections. NWN Carousel will utilize Geo-Blocking mechanisms to ensure the integrity of our network.

### 4.5 Idle Connections

Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. Remote connections to NWN Carousel network must be timed out after 2 hours of inactivity.

### 4.6 Applicability of Other Policies

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics

covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

#### 4.7 **Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

#### 5.0 **Revision History**


Name	Date	Brief Description of Changes	Version
James Aiello	8/26/11	Reformatted Remote Access Policy	Version 1.1
James Aiello	10/31/11	Reformatted Remote Access Policy	Version 1.2
James Aiello	11/9/12	Edited per Information Security Audit	Version 2.0
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.1
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.2
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

#### 6.0 **Approval History**

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methe	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

#### 7.0 **Review Cycle**

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	7/1/12	CIIMT	Completed
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	10/10/21	SRC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-U <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>RETENTION POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that NWN Carousel guidelines on retention are consistently applied throughout the organization.

## 2.0 Scope

The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location.

Note that the need to retain certain information can be mandated by local, industry, or federal regulations. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

## 3.0 Goals

The goal of this policy is to specify NWN Carousel guidelines for retaining different types of data and to ensure that all data is managed and retained in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

## 4.0 Policy

### 4.1 Reasons for Data Retention

NWN Carousel does not wish to simply adopt a "save everything" mentality.

This is not practical or cost-effective, and would place an excessive and unnecessary burden on the business and the CSOIT team to manage the constantly growing amount of data. Some data, however, must be retained in order to protect NWN Carousel interests, preserve evidence, and generally conform to good business practices.

Some reasons for data retention include:

- System Restoration
- Litigation
- Accident investigation
- Security incident investigation
- Regulatory requirements
- Intellectual property preservation
- Auditability
- Financial obligations
- Contracts
- Operational Integrity

### 4.2 Data Duplication

As data storage increases in size and decreases in cost, companies often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's machine, on a central file server, and again on a backup system. When identifying and classifying NWN Carousel data, it is important to also understand where that data may be stored, particularly as duplicate copies, so that this policy may be applied to all duplicates of the information.

### 4.3 Retention Requirements

This section sets guidelines for retaining the different types of company data.

- **Personal** - There are no retention requirements for personal data. In fact, NWN Carousel requires that it be deleted or destroyed when it is no longer needed as quickly as possible.
- **Public** - Public data must be retained for at least 1 year.
- **Operational** - Most company data will fall in this category. Operational data must be retained for at least 2 years.
- **Critical** - Critical data must be retained for at least 3 years.
- **Confidential** - Confidential data must be retained for at least 3 years.
- **Legal** – May not be deleted under any circumstance.

#### 4.4 **Retention of Encrypted Data**

If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

#### 4.5 **Legal Hold**

In the event of litigation or other legal requirements, NWN Carousel can place information on “Legal Hold” in order to meet said judiciary and regulatory requirements. All Legal Holds must be initiated by NWN Carousel Legal Team under the direction of the Chief Financial Officer (CFO) who will notify CSOIT of the specific requirements of the hold. CSOIT will immediately take a snapshot of all applicable databases and store these in a secure location to ensure the information’s integrity. CSOIT will work with any users who are subject to the Legal Hold so that any additional data created is backed up and not deleted per NWN Carousel’s Retention Policy. Once the Legal Hold period is over, the Legal Team will notify CSOIT and all users effected by the hold that the data will once again follow Carousel’s Retention Policy.

#### 4.6 **Data Destruction**

Data destruction is a critical component of a data retention policy. Data destruction ensures that NWN Carousel will not get buried in data, making data management and data retrieval more complicated and expensive than it needs to be. Exactly how certain data should be destroyed is covered in the Data Classification Policy. When the retention timeframe expires, NWN Carousel must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member(s) of the NWN Carousel executive team.

NWN Carousel specifically directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to himself or herself, or destroying data in an attempt to cover up a violation of law or company policy.

#### 4.7 **Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

#### 4.8 **Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

### 5.0 **Revision History**

Name	Date	Brief Description of Changes	Version
James Aiello	8/26/11	Reformatted Retention Policy	Version 1.1
James Aiello	10/31/11	Reformatted Retention Policy	Version 1.2
James Aiello	11/9/12	Edited per Information Security Audit	Version 2.0
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.1
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.2
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

### 6.0 **Approval History**


Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23

Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

**7.0 Review Cycle**

<b>Review Cycle</b>	<b>Scheduled Review Date</b>	<b>Reviewer</b>	<b>Status-Action Needed</b>
Annual	7/1/12	CIIMT	Completed
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	10/10/21	SRC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled



	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-V <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>THIRD PARTY CONNECTION POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

Direct connections to external entities are sometimes required for business operations. These connections are typically to provide access to vendors or customers for service delivery. Since NWN Carousel security policies and controls do not extend to the users of the third parties' networks, these connections can present a significant risk to the network and thus require careful consideration.

## 2.0 Scope

The scope of this policy covers all direct connections to NWN Carousel network from non-company owned networks. For the purpose of this document, “Third Party Connection” is defined as a direct connection to a party external to NWN Carousel. Examples of third party connections include connections to customers, vendors, partners, or suppliers. This policy excludes remote access and Virtual Private Network (VPN) access, which are covered in separate policies.

## 3.0 Goals

The goal of this policy is to provide guidelines for deploying and securing direct connections to third parties.

## 4.0 Policy

### 4.1 Use of Third Party Connections

When it is necessary to grant access to a third party, the access must be restricted and carefully controlled. A requester of a third party connection must demonstrate a compelling business need for the connection. This request must be approved and implemented by CSOIT Team and sign and secure a NWN Carousel Nondisclosure Agreement. (NDA)

### 4.2 Security of Third Party Access

Third party connections require additional scrutiny. The following statements will govern these connections:

- Connections to third parties must use a firewall or Access Control List (ACL) to separate NWN Carousel network from the third party's network.
- Computers and devices of Third Parties may be required to install a corporate approved anti-virus software at the Supervisor of the Corporate Networks discretion.
- Third parties will be provided only the minimum access necessary to perform the function requiring access. If possible this should include time-of-day restrictions to limit access to only the hours when such access is required.
- Wherever possible, systems requiring third party access should be placed in a public network segment or demilitarized zone (DMZ) in order to protect internal network resources.
- If a third party connection is deemed to be a serious security risk, the Director – Security Risk & Compliance will have the authority to prohibit the connection. If the connection is absolutely required for business functions, additional security measures should be taken at the discretion of the Director – Security Risk & Compliance.

### 4.3 Restricting Third Party Access

Best practices for a third party connection require that the link be held to higher security standards than an intra-company connection. As such, the third party must agree to:

- Restrict access to NWN Carousel network to only those users that have a legitimate business need for access.
- Provide NWN Carousel with the names and any other requested information about individuals that will have access to the connection. NWN Carousel reserves the right to approve or deny this access based on its risk assessment of the connection.
- Supply NWN Carousel with on-hours and off-hours contact information for the person or persons responsible for the connection.
- (If confidential data is involved) Provide NWN Carousel with the names and any other requested information about individuals that will have access to NWN Carousel confidential data. The steward or owner of the confidential data will have the right to approve or deny this access for any reason.

### 4.4 Offshore Connections

Connections from outside the continental United States must be afforded extra oversight due to customer

requirements and best practice. The following policy will document the standards that must be in place in order for a resource to connect to the NWN Carousel network from outside the United States:

#### **4.4.a End User Controls**

As offshore employees access NWN Carousel resources from a non-NWN Carousel provided resources, extra diligence must be made to ensure the security of these resources. The devices of External Suppliers connecting to NWN Carousel resources from offshore are expected to be in full compliance with this Information Security Manual. Security, Risk & Compliance Assessments will be performed no less than annually in order to ensure the External Suppliers compliance with NWN Carousel standards and practices.

#### **4.4.b Network Connectivity**

- Source IP's must be restricted to official office locations of External Supplier
- Use of MFA for connection to the VPN is required.
- VPN will only provide direct access to a Jump Server
- Jump Server only provides access to the specific resources on the network for perform their job function
- Each session will be uniquely identified to a single user.
- Each supplier will provided with their own dedicated Jump Server(s).

#### **4.5 Auditing of Connections**

Third Party Connections must be audited quarterly in order to ensure compliance with this policy are in compliance with this policy, they must be audited quarterly.

#### **4.6 Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

#### **4.7 Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

### **5.0 Revision History**

<b>Name</b>	<b>Date</b>	<b>Brief Description of Changes</b>	<b>Version</b>
James Aiello	8/26/11	Reformatted Third Party Connection Policy	Version 1.1
James Aiello	10/31/11	Reformatted Third Party Connection Policy	Version 1.2
James Aiello	7/2/12	Audited Third Party Connection Policy	Version 2.0
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.1
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.2
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1


### **6.0 Approval History**

<b>Approved By</b>	<b>Title</b>	<b>Version Approved</b>	<b>Date Approved</b>
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23

NWN Carousel Security Committee		v3.1	5/19/23
---------------------------------	--	------	---------

**7.0 Review Cycle**

<b>Review Cycle</b>	<b>Scheduled Review Date</b>	<b>Reviewer</b>	<b>Status-Action Needed</b>
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	10/10/21	SRC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-W <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>VIRTUAL PRIVATE NETWORK (VPN) POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

A Virtual Private Network, or VPN, provides a method to communicate with remote sites securely over a public medium, such as the Internet. A site-to-site VPN is a dependable and inexpensive substitute for a point-to-point Wide Area Network (WAN). Site-to-site VPNs can be used to connect the LAN to a number of different types of networks: branch or home offices, vendors, partners, customers, etc. As with any external access, these connections need to be carefully controlled through a policy to mitigate potential security risks.

## 2.0 Scope

The scope of this policy covers all site-to-site VPNs that are a part of NWN Carousel infrastructure, including both sites requiring access to NWN Carousel network (inbound) and sites where NWN Carousel connects to external resources (outbound). Note that remote access VPNs are covered separately in the Remote Access Policy.

## 3.0 Goals

This policy details NWN Carousel standards for site-to-site VPNs. The goal of this policy is to specify the security standards required for such access, ensure the integrity of data transmitted and received, and to secure the VPN pathways into the network.

## 4.0 Policy

### 4.1 Encryption

Site-to-site VPNs must utilize strong encryption to protect data during transmission. Encryption algorithms must meet or exceed the current NWN Carousel standard, which is AES 256 SHA1 Group 5.

### 4.2 Authentication

Site-to-site VPNs must utilize a strong password, pre-shared key, certificate, or other means of authentication to verify the identity the remote entity. At this time site-to-site VPN's must utilize randomly generated 16-character password.

### 4.3 Implementation

When site-to-site VPNs are implemented, they must adhere to the policy of least access, providing access limited to only what is required for business purposes. This must be enforced with a firewall or other access control that has the ability to limit access only to the ports and IP addresses required for business purposes.

### 4.4 Management

NWN Carousel manages its own VPN gateways, meaning that a third party should not provide or manage either side of the site-to-site VPN, unless this arrangement is covered under an External Supplier agreement. If an existing VPN is to be changed, the changes must only be performed with the approval of the CSOIT Senior Management or the Supervisor of the Corporate Network.

### 4.5 Logging and Monitoring

Depending on the nature of the site-to-site VPN, CSOIT Managers will use their discretion as to whether additional logging and monitoring is warranted. As an example, a site-to-site VPN to a third party would likely require additional scrutiny but a VPN to a branch office of NWN Carousel would likely not be subject to additional logging or monitoring. All tunnels to customer sites must be logged for accountability. These logs must be kept for a minimum of 60 days.

### 4.6 Encryption Keys

Site-to-site VPNs are created with pre-shared keys. The security of these keys are critical to the security of the VPN, and by extension, the network. Encryption keys should be changed at a minimum of 24 hours for IKE (Internet Key Exchange) or 8 hours for IPSEC (Internet Protocol Security) relay.

If certificates are used instead of pre-shared keys, they need to be configured to expire and be re-generated for a period not to exceed 3 years.

### 4.7 Applicability of Other Policies

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics

covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

#### 4.8 **Enforcement**

This policy will be enforced by the CSOIT Team and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

#### 5.0 **Revision History**


Name	Date	Brief Description of Changes	Version
James Aiello	8/26/11	Reformatted VPN Policy	Version 1.1
James Aiello	10/31/11	Reformatted VPN Policy	Version 1.2
James Aiello	7/2/12	Audited VPN Policy	Version 2.0
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.1
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.2
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

#### 6.0 **Approval History**

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk & Compliance	v3.1	5/5/23
NWN Carousel Security Committee		v3.1	5/19/23

#### 7.0 **Review Cycle**

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	10/10/21	SRC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled

	<b>NWN Carousel</b> <b>659 South County Trail</b> <b>Exeter, RI 02822</b>	<b>Responsible Group:</b> <i>Customer Success</i>	<b>Number:</b> NC001-X <b>Version:</b> 3.1
		<b>Document Owner:</b> Aiello, James <i>Director – Security Risk &amp; Compliance</i>	<b>Revision Date:</b> 6/6/23
<b>WIRELESS NETWORK POLICY</b>		<b>Approved By:</b> <i>NWN Carousel Security Committee</i>	

## 1.0 Purpose

Wireless communication is playing an increasingly important role in the workplace supporting both mobility and enterprise applications. While wireless access can increase mobility and productivity of users, it also introduces potential security risks to the network. Fortunately, these risks can be mitigated with a sound Wireless Access Policy. The purpose of this policy is to state the standards for NWN Carousel’ wireless networks.

## 2.0 Scope

This policy covers anyone who accesses the network via a wireless connection. The policy further covers the wireless infrastructure of the network, including access points, routers, wireless network interface cards, and anything else capable of transmitting or receiving a wireless signal.

## 3.0 Goals

This document outlines the steps NWN Carousel has taken to secure its wireless infrastructure and enacts policies, which will safeguard the system.

## 4.0 Policy

### 4.1 Physical Guidelines

Unless a directional antenna is used, a wireless access point typically broadcasts its signal in all directions. For this reason, access points must be located central to the office space rather than along exterior walls. If it is possible with the technology in use, signal broadcast strength must be reduced to only what is necessary to cover the office space. Directional antennas should be considered in order to focus the signal to areas where it is needed.

Physical security of access points must be considered. Access points should not be placed in public or easily accessed areas when able. Access points must be placed in non-obvious locations (i.e., above ceiling tiles) so that they cannot be seen or accessed without difficulty.

### 4.2 Configuration and Installation

The following guidelines apply to the configuration and installation of wireless networks:

#### 4.2.a Asset Tracking

All Access Points, RAP’s, switches and firewalls must have an Asset Tag and be entered into the Asset Tracking Database prior to deployment. Each profile must include the model number, software version and licensing details in order to meet business and industry standards.

#### 4.2.b Security Configuration

- The Service Set Identifier (SSID) of the access point must be changed from the factory default. The SSID must be changed to something completely nondescript. Specifically, the SSID must not identify NWN Carousel, the location of the access point, or anything else that may allow a third party to associate the access point’s signal to NWN Carousel.
- Administrative access to wireless access points must utilize strong or hardened passwords. Use of random password generators is recommended.
- Access points should be placed in locations that minimize the risk of interface (away from transmitters, microwave equipment, etc.)
- All of the logging features should be enabled on NWN Carousel access points.

#### 4.2.c Installation

- All network devices, including wireless devices, must be installed by NWN Carousel Converged Support Group (CSOIT) representatives only.
- Software and/or firmware on the wireless access points and wireless network interface cards (NICs) must be updated prior to deployment.
- Wireless networking must not be deployed in a manner that will circumvent NWN Carousel security controls.
- Channels used by wireless devices should be evaluated to ensure that they do not interfere with

company equipment.

#### 4.3 **Inactivity**

Users should disable their wireless capability when not using the wireless network. This will reduce the chances that their machine could be compromised from the wireless NIC. Inactive wireless access points should be disabled. If not regularly used and maintained, inactive access points represent an unacceptable risk to NWN Carousel.

#### 4.4 **Guest Access**

NWN Carousel offers its customers, consultants and vendors access to a secure guest Wi-Fi connection that is separate from the corporate network. Access to this connection is regulated and all guests must register with a NWN Carousel representative to receive a user name and password for access. Employees are restricted from this network and should only be utilizing NWN Carousel' secure corporate wireless network. Please see the Guest Access Policy for more information on this service.

#### 4.5 **Monitoring & Privacy Rights**

Users should have no expectation of privacy when using the corporate electronic communication systems. Such use may include, but is not limited to: transmission and storage of files, data, email and messages. CSOIT is continuously monitoring the corporate network, and by extent, all devices connected to it. This monitoring is done to ensure the integrity of the network and to ensure compliance with established security policies. CSOIT may access any and all information technology resources at any time in accordance with company Information Security Policies.

#### 4.6 **Applicability of Other Policies**

This document is part of NWN Carousel cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, please refer to the Information Security Manual for a complete set of policies.

#### 4.7 **Enforcement**

This policy will be enforced by CSOIT and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, NWN Carousel may report such activities to the applicable authorities.

### 5.0 **Revision History**

Name	Date	Brief Description of Changes	Version
James Aiello	08/16/11	Reformatted Wireless Network Policy	Version 1.3
James Aiello	10/31/11	Reformatted Wireless Network Policy	Version 1.4
James Aiello	12/1/11	Performed CIIMT Audit	Version 2.0
James Aiello	4/14/15	Edited per CIIMT Audit	Version 2.1
James Aiello	8/20/16	Edited per CIIMT Audit	Version 2.2
Jason Albuquerque	12/17/18	Edited per ESC Audit	Version 2.3
Jason Albuquerque	12/20/19	Edited per ESC Audit	Version 2.4
James Aiello	2/14/22	Reformatted for change of ownership & audit results	Version 3.0
James Aiello	5/1/23	Edited per annual audit & TX-RAMP Language	Version 3.1

### 6.0 **Approval History**

Approved By	Title	Version Approved	Date Approved
Jack Lodge	EVP Customer Success	v3.1	6/2/23
Chris Methé	VP Technology Operations	v3.1	5/5/23
James Aiello	Director – Security Risk &	v3.1	5/5/23

	Compliance		
NWN Carousel Security Committee		v3.1	5/19/23

**7.0 Review Cycle**

Review Cycle	Scheduled Review Date	Reviewer	Status-Action Needed
Annual	12/1/11	CIIMT	Performed Information Security Audit
Annual	2/10/15	CIIMT	Completed
Annual	4/1/16	CIIMT	Completed
Annual	8/20/17	CIIMT	Completed
Annual	12/17/18	ESC	Completed
Annual	12/20/19	ESC	Completed
Annual	10/10/21	SRC	Completed
Annual	2/14/22	SRC	Completed
Annual	3/1/23	SRC	Completed
Annual	5/1/24	SRC	Scheduled



## GLOSSARY

- **Access Control List (ACL)**  
A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.
- **Account**  
Combination of a username and password that allows access to computer or network resources.
- **Antivirus Software**  
An application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.
- **Authentication**  
A security method used to verify the identity of a user and authorize access to a system or network.
- **Auto Responder**  
An email function that sends a predetermined response to anyone who sends an email to a certain address. Often used by employees who will not have access to email for an extended period of time, to notify senders of their absence.
- **Backup**  
To copy data to a second location, solely for the purpose of safe keeping of that data.
- **Backup Media**  
Any storage devices that are used to maintain data for backup purposes. These are often magnetic tapes, CDs, DVDs, or hard drives.
- **Biometrics**  
The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.
- **Blogging**  
The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").
- **Business Associate Agreement**  
A business associate agreement is a contract between a company and its associates who will use or may be exposed to protected health information (PHI).
- **Carousel Industries Information Management Team (CIIMT)**  
The CIIMT was the group responsible for designing and implementing the internal Information Management Policies of Carousel Industries from 2011-2016.
- **Customer Success Operations & Information Technology (CSOIT)**  
The Converged Support Group is the combination of the Information Technology (IT) department and the Voice Services group whose primary mission is to deliver, maintain and support all of NWN Carousel employee's technology and application needs.
- **Certificate**  
Also called a "Digital Certificate." A file that confirms the identity of an entity, such as a company or person. Often used in VPN and encryption management to establish trust of the remote entity.
- **Data Center**  
A location used to house a company's servers or other information technology assets. Typically offers enhanced security, redundancy, and environmental controls.
- **Data Leakage**  
Also called Data Loss, data leakage refers to data or intellectual property that is pilfered in small amounts or otherwise removed from the network or computer systems. Data leakage is sometimes malicious and sometimes inadvertent by users with good intentions.
- **Demilitarized Zone (DMZ)**  
A perimeter network, typically inside the firewall but external to the private or protected network, where publicly accessible machines are located. A DMZ allows higher-risk machines to be segmented from the internal network while still providing security controls.
- **Email**  
Short for electronic mail, email refers to electronic letters and other communication sent between networked computer users, either within a company or between companies.
- **Encryption**  
The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.
- **Encryption Key**  
An alphanumeric series of characters that enables data to be encrypted and decrypted.

- **ESC**  
Enterprise Security Team was the group responsible for designing and implementing the internal Information Management Policies of Carousel Industries from 2017-2021.
- **Firewall**  
A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.
- **Full Backup**  
A backup that makes a complete copy of the target data.
- **Guest**  
A visitor to NWN Carousel premises who is not an employee. For the purpose of this document this includes but is not limited to customers, consultants and vendors.
- **SharePoint**  
A collection of SharePoint sites which are the official NWN Carousel Information Management System. The goal is to provide a centralized document management and collaboration portal designed to give teams and business units local management capabilities of their respective information while allowing for enterprise wide consumption via a secure means.
- **HIPPA**  
The Health Insurance Portability and Accountability Act of 1996 was enacted by the United States Congress and signed by President Bill Clinton in 1996 and requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.
- **Instant Messaging**  
A text-based computer application that allows two or more Internet-connected users to "chat" in real time.
- **Incremental Backup**  
A backup that only backs up files that have changed in a designated time period, typically since the last backup was run.
- **Keycard**  
A plastic card that is swiped, or that contains a proximity device, that is used for identification purposes. Often used to grant and/or track physical access.
- **Keypad**  
A small keyboard or number entry device that allows a user to input a code for authentication purposes. Often used to grant and/or track physical access.
- **Malware**  
Short for "malicious software." A software application designed with malicious intent. Viruses and Trojans are common examples of malware.
- **Mobile Data Device**  
A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.
- **Mobile Device**  
A portable device that can be used for certain applications and data storage. Examples include, but are not limited to, tablets, PDAs and Smartphones.
- **Mobile Storage Media**  
A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.
- **Modem**  
A hardware device that allows a computer to send and receive digital information over a telephone line.
- **Network Management**  
A far-reaching term that refers to the process of maintaining and administering a network to ensure its availability, performance, and security.
- **Password**  
A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.
- **PDA**  
Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.
- **PHI**  
Any information about the health status, provision of health care, or payment for health care that can be linked to a specific individual.
- **PII**  
Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

- **Pirated Software**  
Software that has been duplicated and distributed without authorization.
- **Peer-to-Peer (P2P) File Sharing**  
A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.
- **Policy**  
A formal document which defines NWN Carousel' expectations and intentions or decisions reached by management outside of documented policies. The latter are typically issues raised in Managers Meetings, discussed and resolved by a consensus of managers or by decree from the Director of Converged Services. Policy can be considered the rules an organization lives by.
- **Procedure**  
A procedure is a document containing steps that specify how to achieve an activity. Procedures are defined as part of processes. Procedures describe how policy is actually implemented.
- **Process**  
A process is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs and expected results. A process may include any of the roles, responsibilities, tools and management controls required to reliably deliver the outputs.
- **Remote Access**  
The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.
- **Remote Access VPN**  
A VPN implementation at the individual user level. Used to provide remote and traveling users secure network access.
- **Remote Desktop Access**  
Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.
- **Restoration**  
Also called "recovery." The process of restoring the data from its backup-up state to its normal state so that it can be used and accessed in a regular manner.
- **Site-to-Site VPN**  
A VPN implemented between two static sites, often-different locations of a business.
- **Smartphone**  
A mobile telephone that offers additional applications, such as PDA functions and email.
- **Smart Card**  
A plastic card containing a computer chip capable of storing information, typically to prove the identity of the user. A card-reader is required to access the information.
- **Smartphone**  
A mobile telephone that offers additional applications, such as PDA functions and email.
- **Spam**  
Unsolicited bulk email. Spam often includes advertisements, but can include malware, links to infected websites, or other malicious or objectionable content.
- **Split Tunneling**  
A method of accessing a local network and a public network, such as the Internet, using the same connection.
- **SSID**  
Stands for Service Set Identifier. The name that uniquely identifies a wireless network.
- **Standard Operating Procedure (SOP)**  
SOPs detail the regularly recurring work processes that are to be conducted or followed within an organization. They document the way activities are to be performed to facilitate consistent conformance to technical and quality system requirements and to support data quality.
- **Streaming Media**  
Typically audio and/or video files, that can be heard or viewed as it is being delivered, which allows the user to play a clip before the entire download has completed.
- **Timeout**  
A technique that drops or closes a connection after a certain period of inactivity.
- **Third Party Connection**  
A direct connection to a party external to NWN Carousel. Examples of third party connections include connections to customers, vendors, partners, or suppliers

- **Token**  
A small hardware device used to access a computer or network. Tokens are typically in the form of an electronic card or key fob with a regularly changing code on its display.
- **Trojan**  
Also called a "Trojan Horse." An application that is disguised as something innocuous or legitimate, but harbors a malicious payload. Trojans can be used to covertly and remotely gain access to a computer, log keystrokes, or perform other malicious or destructive acts.
- **Two Factor Authentication**  
A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.
- **Uninterruptible Power Supplies (UPSs)**  
A battery system that automatically provides power to electrical devices during a power outage for a certain period of time. Typically also contains power surge protection.
- **Virtual Private Network (VPN)**  
A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.
- **Virus**  
Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.
- **WEP**  
Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.
- **Wi-Fi**  
Short for Wireless Fidelity. Refers to networking protocols that are broadcast wirelessly using the 802.11 family of standards.
- **Wiki**  
A collection websites within the NWN Carousel network that allows the collaborative editing of its content and structure by its users. By definition Wikis are an informal means of information management.
- **Wireless Access Point**  
A central device that broadcasts a wireless signal and allows for user connections. A wireless access point typically connects to a wired network.
- **WPA**  
Stands for Wi-Fi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

# INDEX

- Acceptable Use, 15, 18, 52
- Account, 32, 33, 52, 53, 89
- ACL, 89
- Antivirus Software, 89
- Approval, 15, 18, 22, 25, 28, 34, 36, 39, 41, 44, 48, 51, 54, 62, 65, 67, 72, 75, 77, 79, 87
- Asset Tag, 86
- Audits, 43, 57
- Authentication, 27, 49, 52, 53, 89
- Auto Responder, 89
- Backup, 20, 21, 22, 23, 32, 89
- Biometrics, 69, 89
- Blogging, 89
- Certificate, 89
- CI/IT, 15, 18, 19, 22, 25, 28, 34, 39, 44, 48, 51, 55, 65, 72, 77, 80, 87, 88, 89
- Classification, 23, 24, 25, 26, 32, 49, 79
- Consumer Mobile Devices, 11
- Corporate Technology, 10, 91
- CSOIT, 10, 11, 12, 14, 20, 22, 24, 28, 31, 33, 34, 36, 41, 43, 44, 47, 49, 50, 52, 53, 54, 57, 58, 59, 60, 61, 62, 63, 64, 67, 71, 74, 76, 77, 78, 79, 86, 87, 89
- Data, 12, 20, 23, 24, 26, 27, 28, 31, 32, 33, 38, 46, 49, 69, 78, 79, 89, 90
- Data Center, 89
- Data Leakage, 33, 89
- DMZ, 43, 89
- Email, 10, 11, 29, 30, 31, 32, 33, 34, 38, 89
- Encryption, 27, 38, 39, 50, 54, 79, 89
- Encryption Key, 38, 89
- ESC, 15, 19, 22, 25, 28, 34, 39, 41, 42, 44, 48, 51, 54, 55, 62, 65, 71, 72, 75, 77, 79, 80, 82, 83, 85, 87, 88, 90
- Firewall, 60, 90
- Full Backup, 90
- Guest, 43, 44, 59, 87, 90
- HIPPA, 74, 90
- Incremental Backup, 90
- Information Security Awareness Program, 74
- Instant Message, 11
- Instant Messaging, 11, 30, 90
- Issued Technology, 10
- Keycard, 90
- Keypad, 90
- Laptops, 49
- Malware, 60, 90
- Mobile Data Device, 90
- Mobile Device, 49, 50, 51, 69, 90
- Mobile Storage Media, 24, 26, 50, 90
- Modem, 90
- Monitoring, 14, 31, 33, 36, 43, 50, 70, 87
- Network, 10, 12, 13, 27, 43, 49, 50, 52, 53, 56, 58, 59, 60, 62, 69, 76, 87, 90, 92
- Network Access, 10, 43, 49, 50, 52, 53, 76
- Network Management, 90
- P2P, 14, 91
- Password, 10, 31, 49, 52, 53, 65, 90
- PDA, 45, 90, 91
- PHI, 73, 74, 89, 90
- PII, 73, 74, 90
- Pirated Software, 91
- Policy, 10, 12, 14, 15, 18, 22, 23, 24, 25, 26, 27, 28, 29, 31, 32, 34, 38, 39, 40, 41, 43, 44, 45, 48, 49, 50, 51, 52, 53, 54, 56, 57, 60, 61, 62, 63, 65, 68, 69, 71, 73, 76, 77, 78, 79, 86, 87, 91
- Procedure, 91
- Process, 91
- Prohibited, 12, 33, 76
- Remote Access, 12, 53, 91
- Remote Access VPN, 91
- Remote Desktop Access, 12, 91
- Restoration, 21, 91
- Risk, 47, 59, 69
- Security, 10, 11, 12, 14, 27, 30, 34, 36, 40, 43, 49, 58, 60, 61, 62, 68, 69, 70, 73, 78, 86, 87, 88
- SharePoint, 90
- Site-to-Site VPN, 91
- Smart Card, 91
- Smartphone, 45, 91
- Smartphones, 49, 90
- SOP, 91
- Spam, 91
- Split Tunneling, 76, 91
- SSID, 43, 86, 91
- Streaming Media, 12, 91
- Tablets, 49
- Third Party Connection, 91
- Timeout, 91
- Token, 92
- Trojan, 14, 45, 92
- Two Factor Authentication, 92
- Uninterruptible Power Supplies (UPSs), 70, 92
- Virtual Private Network (VPN), 92
- Virus, 92
- VPN, 38, 41, 89, 91, 92
- WEP, 46, 92
- Wi-Fi, 87, 92
- Wiki, 92
- Wireless Access Point, 92
- WPA, 46, 92

## CHANGE MANAGEMENT LOG

<b>Policy Name</b>	<b>Document ID#</b>	<b>Last Audited</b>	<b>Last Revised</b>	<b>Current Version</b>
<b>Corporate Security Policy: Vision, Philosophy and Enforcement</b>	NC001-A	4/5/23	6/6/23	Version 1.1
<b>Acceptable Use Policy</b>	NC001-B	4/5/23	6/6/23	Version 3.1
<b>Asset Management Policy</b>	NC001-C	4/5/23	6/6/23	Version 3.1
<b>Backup Policy</b>	NC001-D	4/5/23	6/6/23	Version 3.1
<b>Classification Policy</b>	NC001-E	4/5/23	6/6/23	Version 3.1
<b>Confidential Data Policy</b>	NC001-F	4/5/23	6/6/23	Version 3.1
<b>Electronic Communications Policy</b>	NC001-G	4/5/23	6/6/23	Version 3.1
<b>Employee Administration Policy</b>	NC001-H	4/5/23	6/6/23	Version 3.1
<b>Encryption Policy</b>	NC001-I	4/5/23	6/6/23	Version 3.1
<b>External Supplier Management Policy</b>	NC001-J	4/5/23	6/6/23	Version 3.1
<b>Guest Wireless Network Policy</b>	NC001-K	4/5/23	6/6/23	Version 3.1
<b>Incident Response Policy</b>	NC001-L	4/5/23	6/6/23	Version 3.1
<b>Mobile Device Policy</b>	NC001-M	4/5/23	6/6/23	Version 3.1
<b>Network Access &amp; Authentication Policy</b>	NC001-N	4/5/23	6/6/23	Version 3.1
<b>Network Security Policy</b>	NC001-O	4/5/23	6/6/23	Version 3.1
<b>Password Policy</b>	NC001-P	4/5/23	6/6/23	Version 3.1
<b>Patch Management Policy</b>	NC001-Q	4/5/23	6/6/23	Version 3.1
<b>Physical Security Policy</b>	NC001-R	4/5/23	6/6/23	Version 3.1
<b>Privacy Policy</b>	NC001-S	4/5/23	6/6/23	Version 3.1
<b>Remote Access Policy</b>	NC001-T	4/5/23	6/6/23	Version 3.1
<b>Retention Policy</b>	NC001-U	4/5/23	6/6/23	Version 3.1
<b>Third Party Connection Policy</b>	NC001-V	4/5/23	6/6/23	Version 3.1
<b>VPN Policy</b>	NC001-W	4/5/23	6/6/23	Version 3.1
<b>Wireless Network Policy</b>	NC001-X	4/5/23	6/6/23	Version 3.1