DATA PROCESSING AGREEMENT

Last Updated: October 30, 2026

This Data Processing Agreement ("DPA") is between NWN Corporation, Carousel Industries of North America, LLC, InterVision Systems, LLC, and Leverage Information Systems, Inc. (collectively, "NWN" or "we") and you or the entity that you represent (collectively, "you") and is incorporated into and governed by the applicable master services agreement or other agreement you entered into with NWN for the provision of services (the "Services") by NWN to you, together with the Quotes and Scopes of Work issued thereunder (the "Service Agreement"). This DPA applies to the extent that we process Personal Data (as defined below) on your behalf while providing the Services under the Service Agreement and sets out the rights and obligations of you and NWN with respect to our processing Personal Data in our capacity as your processor or service provider under the Service Agreement. This DPA will remain in full force and effect so long as NWN retains Personal Data related to the Service Agreement in its possession or control. For avoidance of doubt, the NWN affiliate entity in which you entered your Service Agreement is the contracting entity to this DPA and all other NWN affiliates listed above are not parties to this DPA and shall not be jointly and severally liable for any obligations or liabilities of the contracting NWN affiliate to the Service Agreement.

PLEASE READ THESE TERMS AND CONDITIONS VERY CAREFULLY

1. Interpretation and Definitions.
   The Schedules form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Schedules. If there is any inconsistency or conflict between the terms of the Service Agreement and this DPA as it relates to the processing of Personal Data on your behalf by NWN, this DPA shall prevail. If there is any inconsistency or conflict between this DPA and any executed Standard Contractual Clauses as it relates to the processing of Personal Data on your behalf by NWN, the provisions of the executed Standard Contractual Clauses will prevail. The following definitions and rules of interpretation apply in this DPA.

   1.1 "controller," "business," "processor," "subprocessor" "service provider," "data subject," "consumer," "process," "sale," "sell," "business purpose," and "supervisory authority" (or any equivalent terms) have the meaning set out under the applicable Data Protection Laws.

   1.2 "California Consumer Privacy Act" or "CCPA" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act (CPRA) (Cal. Civ. Code § 1798.100 et seq), the CCPA Regulations (Cal. Code Regs. tit. 11, §§ 7000 to 7102), and any related regulations or guidance provided by the California Attorney General or California Privacy Protection Agency.

   1.3 "European Data Protection Laws" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as amended or superseded from time to time ("EU GDPR"); the EU GDPR as it forms part of the law of the United Kingdom by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (together, "UK Data Protection Laws"); and the Swiss Federal Act on Data Protection of 25 September 2020 (as in force from 1 September 2023) and its ordinances ("Swiss DPA").

   1.4 "Data Protection Laws" means applicable laws governing the privacy and security of Personal Data, including, where applicable, and without limitation, European Data Protection Laws, the CCPA, the Health Insurance Portability and Accountability Act of 1996, as amended, and its implementing regulations ("HIPAA"), and other U.S. state comprehensive consumer privacy laws.

1.5 “Permitted Purpose” means processing of Personal Data (i) as necessary for the provision of the Services as set forth in greater detail in Schedule 1; (ii) as otherwise permitted by Data Protection Laws in connection with the Services; and (iii) to comply with legal obligations which do not conflict with Data Protection Laws.

1.6 “Personal Data” means any information that identifies relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household in connection with the Services performed for you, including without limitation any information that qualifies as “personal information” or “personal data” under the Data Protection Laws applicable to NWN.

1.7 “Restricted Transfer” means (i) where EU GDPR or the Swiss DPA applies, a transfer of Personal Data from the European Economic Area (“EEA”) including Switzerland to a country outside of the EEA, which is not the subject of an adequacy determination by the European Commission; and (ii) where UK GDPR applies, a transfer of Personal Data from the United Kingdom to any country which is not subject to adequacy regulations pursuant to Section 17A of the UK Data Protection Act.

1.8 “Security Breach” means a breach of security leading to unauthorized disclosure of or access to Personal Data in NWN’s possession, custody or control.

1.9 “Sensitive Data” means (a) social security number, tax file number, passport number, driver’s license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, credit, genetic, biometric or health information, including protected health information as defined under HIPAA; (d) racial, ethnic, political or religious affiliation, trade union membership, information about sexual life or sexual orientation, or criminal record; (e) account passwords; or (f) other information that falls within the definition of “special categories of data,” “sensitive data” or “nonpublic personal information” under applicable Data Protection Laws or personal information as defined in appliable data breach notification laws.

1.10 “Standard Contractual Clauses” means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission’s Implementation Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to the EU GDPR (“EU SCCs”); (ii) where the Swiss DPA applies, the EU SCCs as adapted in Schedule 2, Section 2; and (iii) where the UK Data Protection Laws apply, the UK Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner’s Office under s.119A(1) of the Data Protection Act 2018 (the “UK Addendum”).

2. Scope of DPA.

2.1 For the avoidance of doubt, it is the intention of both you and NWN that we be a “service provider,” “processor” or “licensee” of you when required by applicable Data Protection Laws and you be a “business,” “controller” or “licensor” when required by applicable Data Protection Laws.

2.2 You instruct us to, and NWN will only process, retain, use, or disclose Personal Data for the Permitted Purpose. We will promptly notify you if, in our opinion, your instruction would not comply with the Data Protection Laws. If a law requires us to disclose Personal Data for a purpose unrelated to the Permitted Purpose, we will inform you of the legal requirement and give you an opportunity to object or challenge the requirement, unless the law prohibits such notice.

2.3 You acknowledge and agree that we will not be required to process any Sensitive Data on your behalf unless explicitly stated in a Service Agreement, in which case you will identify the categories and types of Sensitive Data which will be the subject of the processing in the applicable Service Agreement. Unless the Parties agree that NWN will process Sensitive Data on your behalf in a Service Agreement, you will restrict our access to any Sensitive Data under its possession or control.

2.4 If NWN will create, receive, maintain, or transmit protected health information subject to HIPAA on your behalf, the parties must first execute a separate business associate agreement, and you will not provide any such information to NWN until that agreement is in effect.

2.5 If any Data Protection Law imposes additional or overriding obligations to those set forth in this DPA with respect to processing of Personal Data or requires you and NWN to enter into any additional agreements to process Personal Data under the DPA, you shall ensure that you comply with the applicable Data Protection Law in advance of disclosing any Personal Data subject to such Data Protection Laws and you and NWN agree to negotiate such additional obligations, agreements, or security measures in good faith.

3. Personal Information Types and Processing Purposes.
You retain control of the Personal Data and remain responsible for complying with your obligations under the applicable Data Protection Laws, including providing any required notices and obtaining any required consents, and for the processing instructions you provide to us. Schedule 1 describes the general Personal Data categories and related types of data subjects NWN may process to fulfill the Permitted Purpose of the Service Agreement. You warrant and represent that NWN's expected use of the Personal Data for the Permitted Purpose and as specifically instructed by you will comply with all Data Protection Laws.

4. Our Obligations.

4.1 NWN shall:

(a) promptly comply with your request or instruction to amend, transfer, or delete the Personal Data, or to stop, mitigate, or remedy any unauthorized processing, to the extent within the scope of the Services and technically feasible, provided that requests requiring effort beyond the Services may be subject to reasonable additional fees;

(b) maintain the confidentiality of all Personal Data, will not sell it to or share it for cross-contextual advertising with anyone, and will not disclose it to third parties unless your or this DPA specifically authorizes the disclosure, or as required by law;

(c) limit Personal Data access to those employees who require Personal Data access to meet our obligations under this DPA and the Service Agreement; and the part or parts of the Personal Data that those employees strictly require for the performance of their duties;

(d) take reasonable steps to ensure the reliability, integrity, and trustworthiness of all of our employees with access to the Personal Data;

(e) ensure that all employees are informed of the Personal Data's confidential nature and use restrictions and are obliged to keep the Personal Data confidential, have undertaken training on the Data Protection Laws relating to handling Personal Data and how it applies to their particular duties; and are aware both of NWN's

duties and their personal duties and obligations under Data Protection Laws and this DPA;

(f) reasonably assist you with meeting your compliance obligations under the Data Protection Laws, taking into account the nature of our processing and the information available to us;

(g) keep appropriate documentation of its processing activities as required by Data Protection Laws; and

(h) promptly notify you if we determine that we can no longer meet our obligations under applicable Data Protection Laws or this DPA.

4.2 You acknowledge that we are under no duty to investigate the completeness, accuracy, or sufficiency of your instructions or the Personal Data other than as required under Data Protection Laws.

5. Security

Taking into account the nature of our processing, NWN will implement appropriate technical and organizational measures designed to safeguard Personal Data against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, destruction, unavailability, or damage including, but not limited to, the security measures set out in Schedule 3. We will notify you if we become aware of any advance in technology and methods of working, which indicate that the parties should adjust their security measures. NWN will take reasonable precautions to preserve the integrity of any Personal Data it stores and processes and to prevent any corruption or loss of such Personal Data, including but not limited to establishing effective back-up and data restoration procedures. We will notify you only if our implementation of alternative security measures results in a material diminution of the security of our overall information security program.

6. Security Breaches and Personal Information Loss

NWN will notify you without undue delay after NWN confirms a Security Breach. We will reasonably cooperate in the investigation of the Security Breach. If and to the extent that the Security Breach is proximately caused by our failure to comply with this DPA, NWN will reimburse you for your documented and reasonable out-of-pocket costs of providing notifications legally required under applicable Data Protection Laws, which reimbursement shall be subject to the limitations of liability in the Service Agreement, unless the matter arose from your specific instructions, negligence, willful default, or breach of this DPA, in which case you will cover all expenses. NWN agrees that you have the sole right to determine whether to provide notice of the Security Breach to any data subjects, regulators, law enforcement agencies, or others, as required by law or regulation or in your discretion, including the contents and delivery method of the notice.

7. Cross-Border Transfers of Personal Information.

If and to the extent that performance of any Services requires the transfer of Personal Data from you to NWN which is a Restricted Transfer, you will only transfer that Personal Data to us if NWN, either through our location or participation in a valid cross-border transfer mechanism under the European Data Protection Laws, as identified in Schedule 1, may legally receive that Personal Data, provided that NWN informs you of any change to that status.

8. Subcontractors.

You agree that NWN has your general authorization to subcontract its obligations to third parties (subcontractors or subprocessors) to process Personal Data as necessary to perform the Services under the Service Agreement to those parties identified in Schedule 1. NWN shall inform you of any intended addition or replacement of subprocessors at least thirty (30)

days in advance, which notice may be given by updating the subprocessor list at https://nwn.ai/compliance/ and notifying you (including by email or through a subscription mechanism). You may object to a new subprocessor on reasonable data-protection grounds by written notice within that period, in which case the parties will discuss your concerns in good faith. NWN shall enter into a written contract with the subcontractor that are at least as protective of Personal Data as those reflected in this DPA. Should a subcontractor fail to fulfill its obligations under such written agreement, NWN remains fully liable to you for the subcontractor's performance of its agreement obligations. NWN shall ensure that any subcontractors who have access to Personal Data are bound to process Personal Data in accordance with our instructions and are subject to obligations to maintain confidentiality.

9. Complaints, data subject Requests, and Third-Party Rights. NWN will:

9.1 promptly notify you if it receives any complaint, notice, or communication that directly or indirectly relates to the Personal Data processing or to either party's compliance with Data Protection Laws;

9.2 promptly notify you if we receive a request from a data subject to exercise any rights the individual may have regarding their Personal Data, such as access, correction, deletion, or to opt-out of or limit certain activities like sales, disclosures, or other processing actions;

9.3 reasonably cooperate and assist you in responding to any complaint, notice, communication, or data subject; and

9.4 not disclose the Personal Data to any data subject or to a third party unless the disclosure is either at your request or instruction, permitted by this DPA, or is otherwise required by law.

10. Data Return and Destruction.
On termination of the Service Agreement for any reason or expiration of its term, upon your written request made within thirty (30) days after such termination or expiration, NWN will, at your election, securely return or destroy, and not retain, all or any Personal Data related to this DPA in its possession or control, unless required by law, rule or regulation, or requested by any judicial, administrative, governmental or regulatory authority to retain the Personal Data or if return or destruction would otherwise involve disproportionate efforts under the circumstances. After Personal Data has been deleted from our active systems, it may continue to exist in backups and logs for a period of time until these are overwritten in the normal course of business and in accordance with our data retention and destruction policies.

11. Audit

11.1 Reviews of Security Documentation. To demonstrate NWN's compliance with its obligations under this DPA, upon your written request on an annual basis (other than in the event of a Security Breach) we will provide customer-facing documentation on the current state of our information security program and/or third-party certification or security assessment documentation.

11.2 Audit Rights. To the extent required by Data Protection Laws, we will allow you to conduct, and will reasonably cooperate with, no more than once per calendar year, audits/inspections to verify NWN's compliance with its obligations under this DPA, subject to the limitations set forth in this paragraph. You must contact the NWN Security Team at security@nwn.ai to request an audit. Following this request, NWN and you will discuss and agree in advance on any security and confidentiality obligations, a reasonable start date, the scope and duration, and any applicable fees. NWN may object to any third-

party auditor you appoint to conduct the audit if in our reasonable opinion, the auditor is not appropriately qualified, suited, or independent.

12. CCPA Compliance.
Both parties will comply with all applicable requirements of the CCPA when collecting, using, retaining, or disclosing Personal Data. With respect to Personal Data collected about California residents that is governed by the CCPA, NWN:

12.1 will not collect, use, retain, disclose, sell, or otherwise make Personal Data available for NWN's own commercial purposes or in a way that does not comply with the CCPA;

12.2 will limit Personal Data collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the Permitted Purpose or another compatible operational purpose.

12.3 if the Permitted Purpose requires the collection of Personal Data from individuals on your behalf, we will always provide a CCPA-compliant notice at collection that you specifically pre-approve;

12.4 certifies that it understands this DPA and the CCPA's restrictions and prohibitions on selling personal information and retaining, using, or disclosing personal information outside of the parties' direct business relationship, and it will comply with them; and

12.5 warrants that it has no reason to believe any CCPA requirements or restrictions prevent it from providing any of the Services or otherwise performing under this DPA. NWN must promptly notify you of any changes to the CCPA's requirements that may adversely affect its performance under this DPA.

12.6 grants you the right, upon notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data by NWN.

If the CCPA permits, we may aggregate, deidentify, or anonymize personal information so it no longer meets the personal information definition, and may use such aggregated, deidentified, or anonymized data for any purpose permitted under applicable law, including, without limitation, its own research and development purposes; provided that such use complies with the restrictions on AI Training in any AI Addendum between the parties and does not identify you. NWN will not attempt to or actually re-identify any previously aggregated, deidentified, or anonymized data and will contractually prohibit downstream data recipients from attempting to or actually re-identifying such data.

13. Integration. This DPA, including the Standard Contractual Clauses, and the Service Agreement constitute the parties' entire agreement and understanding with respect to the subject matter hereof. The obligations contained in this DPA are (i) subject to any limitations of liability set forth in the Service Agreement and are (ii) in addition to other obligations contained in the Service Agreement.

SCHEDULE 1-PERSONAL INFORMATION PROCESSING PURPOSES AND DETAILS

A. THE PARTIES	
Data Exporter/Controller	
Name:	As set forth in the applicable Service Agreement
Address:	As set forth in the applicable Service Agreement or otherwise provided to Data Importer

Contact Information:	As set forth in the applicable Service Agreement or otherwise provided to Data Importer
Activities relevant to the data:	See Section B
Data Importer/Processor	
Name:	The NWN entity that is party to the Service Agreement
Address:	659 South County Trail Exeter, RI 02822
Contact Information:	Legal Department. compliance-legal@nwn.ai
Activities relevant to the data:	See Section B
Description of Processing/Transfer	
Subject Matter, Nature and Purpose of Processing	Processing as reasonably necessary and proportionate to perform the Services on Data Exporter's behalf pursuant to the applicable Service Agreement for business purposes and in accordance with the DPA. The foregoing includes project based professional and managed Services (including, but not limited to, configuration, implementation, assessment, staff augmentation, unified communications, hosted and network services) maintaining or servicing accounts, providing storage and other types of processing of Personal Data as necessary to provide the Services.
Categories of Data Subjects:	Data Exporter's employees, contractors, customers, and other individuals whose Personal Data is processed through the Services (such as end users, callers, and meeting or contact-center participants)
Types of Personal Data	Name, address (physical), email, phone number, IP address, system access/usage/authorization data, other non-Sensitive Data No processing of Sensitive Data or any special categories is intended; if and to the extent that processing of the foregoing are necessary under the Service Agreement, then the parties will update the applicable Service Agreement. Data Exporter is solely responsible for determining and notifying Data Importer of such processing and additional restrictions and/or security measures (if any) that are needed to be applied to the Sensitive Data transferred by Data Exporter.
Duration	Continuously for the term of the Service Agreement plus the limited time following its termination in accordance with Section 10 of the DPA.
Restricted Transfers	
NWN's legal basis for receiving Personal Data with cross-border transfer restrictions (select one):	☐ Located in an EEA Member State or in a country with a current determination of adequacy (list country): _____ ☐ Binding Corporate Rules x Standard Contractual Clauses ☐ Other (describe in detail):_____
Subprocessors:	
	Third-party personnel who are natural persons engaged by NWN to assist the delivery of the Services described in the Services Agreement. A current list of approved subprocessors is set forth https://nwn.ai/compliance/. Additional NWN Subcontractors engaged to perform Services as permitted under the Service Agreement.

SCHEDULE 2: STANDARD CONTRACTUAL CLAUSES FOR THE EUROPEAN UNION, SWITZERLAND, AND THE UNITED KINGDOM

1. EU Standard Contractual Clauses. With respect to Personal Data transferred from the European Union governed by the GDPR, you and NWN agree that the EU SCCs are hereby incorporated by reference into this DPA in accordance with the provisions below:

   1.1 Module 2 shall apply;

   1.2 Clause 7 (Docking Clause) shall apply;

   1.3 In Clause 9(a) (Use of sub-processors) – Option 2 shall apply, and the time period for prior notice of Sub-processor changes shall be at least thirty (30) calendar days in advance of such change;

   1.4 In Clause 11(a) (Redress) – the optional provision shall NOT apply;

   1.5 For purposes of Clause 13, the competent supervisory authority shall be determined in accordance with Clause 13(a) of the EU SCCs, and where Data Exporter is not established in the EU and has not appointed a representative, the Irish Data Protection Commission shall act as competent supervisory authority;

   1.6 In Clause 17 (Governing law), Option 1 shall apply and the laws of Ireland shall govern, and in Clause 18(b) (Choice of forum and jurisdiction), disputes shall be resolved before the courts of Ireland;

   1.7 Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 of the DPA;

   1.8 Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 3 of the DPA; and

   1.9 where Module Two (Transfer controller to processor) applies, Annex III of the EU SCCs shall be deemed completed with the information set out in Schedule 1.

   Notwithstanding the fact that the SCCs are incorporated herein by reference without being signed directly, NWN and you each agree that their execution of the Service Agreement is deemed to constitute its execution of the SCCs as of the date thereof, and that it is duly authorized to do so on behalf of, and to contractually bind, the Data Exporter or Data Importer (as applicable) accordingly.

2. Swiss Standard Contractual Clauses. With respect to Personal Data transferred from Switzerland governed by Swiss law, you and NWN agree that the EU SCCs are hereby incorporated by reference into this DPA in accordance with the provisions in section 1 of this Schedule 2, as amended by the provisions below:

   2.1 references to the EU, member states and GDPR in the SCCs are amended mutatis mutandis to refer to Switzerland, the Swiss DPA (as it may be updated or replaced from time to time), and the Swiss Federal Data Protection and Information Commissioner; and

   2.2 in Clause 17 (Governing Law) the laws of Switzerland shall govern, and in Clause 18 (Choice of forum and jurisdiction) the courts of Switzerland shall have jurisdiction.

3. United Kingdom Standard Contractual Clauses. With respect to Personal Data transferred from the United Kingdom governed by UK law, you and NWN agree that the EU SCCs are hereby incorporated by reference into this DPA in accordance with the provisions in section 1 of this Schedule 2, as amended by the template International Data Transfer Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2

February 2022, as it may be revised from time to time (the "UK Addendum") and by the provisions below:

3.1 References to the "Clauses" means the UK Addendum;

3.2 the information required by Tables 1 – 3 of the UK Addendum is provided in the Service Agreement, DPA, and Schedules to the DPA;

3.3 References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

3.4 References to Regulation (EU) 2018/1725 are removed;

3.5 References to the EU, member states and GDPR in the Standard Contractual Clauses are amended to refer to the United Kingdom, the UK Data Protection Act 2018 (as it may be updated or replaced from time to time), and the UK Information Commissioner's Office (the "ICO");

3.6 In Clause 17 (Governing Law), the laws of England and Wales shall govern, and in Clause 18 (Choice of forum and jurisdiction), the courts in London, England shall have jurisdiction and a data subject may also bring legal proceedings against the data exporter and/or data importer before appropriate courts in England and Wales;

3.7 If there is any inconsistency or conflict between UK Data Protection Laws (including the UK Addendum) and the SCCs including this UK Addendum, UK Data Protection Laws including the UK Addendum will govern data transfers from the United Kingdom; and

3.8 To the extent required by UK Data Protection Laws the UK Addendum is incorporated herein.

SCHEDULE 3- SECURITY MEASURES

NWN implements and maintains appropriate technical, organizational and physical safeguards designed to protect against the unauthorized processing and against accidental loss, destruction, damage, disclosure or alteration of your Personal Data in our custody or control, including, the following:

1. Security Policies**.** NWN implements and maintains a comprehensive, written information security program, aligned to industry standards and that contains appropriate administrative, technical, and physical safeguards designed to protect the security, confidentiality, or integrity of Personal Data in our custody or control ("Information Security Program") that meets or exceeds the requirements of these Security Measures and applicable law. NWN reviews and, as necessary, revises its Information Security Program at least annually and will notify its customers if changes to the program negatively impact the level of security provided.

2. Data Access Controls. NWN restricts physical and logical access to Personal Data in our custody or control to only those necessary for the provision of Services through the use of various access controls, including:

- monitoring and logging physical and logical access to NWN's systems that contain Personal Data;
- reviewing successful and failed access attempts for systems that contain Personal Data to identify potentially malicious activity;
- ensuring personnel accessing systems that store Personal Data use unique individual access credentials that meet industry standards for password strength; and
- maintaining a formal program for the periodic review of access and removal of access to for those personnel that no longer require access.

3. System Access Controls. NWN maintains system access controls that meet industry standards for:

    - firewall and network architecture, including considerations for internal and external communications;
    - intrusion detection and prevention;
    - encryption for data both at rest and in motion;
    - segmentation, ensuring Personal Data is logically separated from NWN's and its other customers' data;
    - device hardening and standard configuration, including the removal of system defaults and unused ports and services;
    - malware detection and prevention designed to protect NWN's systems, including those that store Personal Data or connect to customer environments; and
    - security event monitoring, including alerting, response, remediation, and log protection and retention procedures.

4. Training. NWN provides its employees with access to Personal Data with appropriate periodic information security education and awareness training.

5. Security Monitoring. NWN implements industry standard controls to detect or prevent unauthorized devices from connecting to the network that provides Services, including:

    - vulnerability awareness, including industry awareness and regular vulnerability scans and penetration testing;
    - vulnerability management, including patch management; and
    - security incident response plans for the identification, escalation, mitigation, and resolution of suspected security incidents.

6. Security Standards. NWN implements appropriate security measures in compliance with applicable data security laws. Depending on the Services NWN provides, NWN will maintain safeguards such as SOC 1 and SOC 2 reports produced by a third-party auditor and updated annually based on an audit performed at least once every 12 months.