Written Information Security Policies

Table of Contents

1) Overview

Mavis's Machine Shops (the "Company") has developed and is implementing this Written Information Security Plan ("WISP") to ensure effective procedural, administrative, technological and physical safeguards for protecting the Nonpublic Information, including without limitation Personally Identifiable Information, about or provided by the Company's employees and clients. These protections are designed to meet or exceed those required by 73 PA. STAT. §§ 2301 – 2308 & 2329, N.J. Stat. § 56:8-163, 23 NYCRR 500, the California Consumer Privacy Act ("CCPA") and other relevant state or federal laws. This WISP sets forth the Company's procedures for evaluating its electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting Nonpublic Information, as defined below.

2) WISP Objectives

In formulating and implementing this WISP, the Company seeks to create a cybersecurity program which is based on the Company's Risk Management Plan and is designed to perform the following core cybersecurity and data privacy functions:

(1) Protect the confidentiality, integrity, and availability of the Company's Information Systems containing Nonpublic Information;
(2) Identify reasonably foreseeable and likely internal and external risks that may threaten the security or integrity of electronic, paper, or other records containing Nonpublic Information;
(3) Assess the likelihood and potential damage of the risks, taking into consideration the sensitivity of the Nonpublic Information;
(4) Design and implement a plan that puts safeguards in place to minimize the risks, consistent with the Company's legal and regulatory obligations;
(5) Evaluate the sufficiency of existing policies, procedures, Company Information Systems, and other safeguards in place to control risks;
(6) Use defensive infrastructure and the implementation of policies and procedures to protect the Company's Information Systems and/or the Nonpublic Information stored on those Information Systems from unauthorized access, use or other malicious acts;
(7) Regularly monitor the effectiveness of those safeguards;
(8) Identify and detect Cybersecurity Events and respond to such events to mitigate negative effects to the extent possible;
(9) Recover from cybersecurity events and restore normal operations and services; and
(10) Fulfill applicable regulatory reporting obligations.

3) Definitions

1. Authorized User

Authorized user means any employee, contractor, agent, or other person that participates in the business operations of the Company and is authorized to access and use any of the Company's Information Systems or Nonpublic Data.

2. Breach

Breach means the accidental or unlawful alteration, unauthorized disclosure of, or access to, unencrypted PII or encrypted electronic PII along with the confidential decryption process or key that is capable of compromising the

confidentiality or integrity of PII maintained by the Company and thereby creating a substantial risk of identity theft or fraud against the PII Subject. A "Breach" shall not include disclosure of Public Information or where disclosure is required by court order or where necessary to comply with state or federal regulations. For the purposes of clarity, a good faith but unauthorized acquisition of PII by a person, for the lawful purposes of such person, is not a Breach unless the PII is used in an unauthorized manner or subject to further unauthorized disclosure.

3. Cybersecurity Event

Cybersecurity Event means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse an information system or information stored on such information system including, without limitation, a Breach.

4. Data Security Manger

The Company has identified the Company's Managing Partner as the Data Security Manager.

5. Data Security Coordinator

The Company has identified the Company's Office Manager as the Data Security Coordinator.

6. Information System

Information System means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

7. Least Privilege

The principle of Least Privilege requires that each user account, processes, system, device, etc. within the computing environment can only access the information and resources that are necessary for its legitimate purpose.

8. Multi-factor Authentication

Multi-factor Authentication means authentication through verification of at least two of the following types of authentication factors:

(1) knowledge factors, such as a password;
(2) possession factors, such as a token or text message on a mobile phone; or
(3) inherence factors, such as a biometric characteristic.

9. Nonpublic Information

Nonpublic Information means all electronic information that is not Publicly Available Information and is:

(1) business related information of a client the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the client;
(2) Personally Identifiable Information; or,
(3) any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to:
    a. the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family;
    b. the provision of health care to any individual; or
    c. payment for the provision of health care to any individual.

10. Penetration Testing

Penetration testing means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Company's information systems.

11. Person

Person means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.

12. Personally Identifiable Information

The terms PII and Personally Identifiable Information mean any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements:

(1) social security number;
(2) drivers' license number or non-driver identification card number;
(3) account number, credit or debit card number;
(4) any security code, access code or password that would permit access to an individual's financial account; or
(5) biometric records.

13. PII Subject

PII Subject means the person about whom the Personally Identifiable Information pertains.

14. Publicly Available Information

Publicly Available Information means any information that the Company has a reasonable basis to believe is lawfully made available to the general public from: Federal, State or local government records; widely distributed media, including the Internet; or disclosures to the general public that are required to be made by Federal, State or local law. For the purposes of this WISP, the Company has a reasonable basis to believe that information is lawfully made available to the public if the Company has taken steps to determine:

(1) that the information is of the type that is available to the general public; and
(2) whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

15. Risk-based Authentication

Risk-based Authentication means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a person and requires additional verification of the person's identity when such deviations or changes are detected, such as through the use of challenge questions.

16. Senior Officers

Senior officer(s) means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of the Company.

17. Third-party Service Provider(s)

Third party service provider(s) means a person that:

(1) is not an affiliate of the Company;
(2) provides services to the Company; and

(3) maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to the Company.

18. Vulnerability Assessment

A vulnerability assessment means identifying, quantifying, and prioritizing (or ranking) vulnerabilities existing in the Company's Information Systems.

19. WISP

The term WISP refers to this Written Information Security Plan.

4) Responsible Parties and Responsibilities

1. Chief Information Security Officer

The Company shall appoint an individual (the "Chief Information Security Officer" or "CISO" for the purposes of this WISP) who shall be responsible for:

- Implementing the Safeguards and Procedures defined in this WISP;
- Implementing other safeguards reasonably deemed necessary by the CISO, consistent with the Company's Risk Management Plan and this WISP; and,
- Providing to the Data Security Manager an annual certification of the Company's Cybersecurity Program consistent with this WISP.

For the purposes of clarity, the CISO may be a Third-party Service Provider.

2. Data Security Manager Responsibilities:

The Data Security Manger shall be responsible for:

- Ensuring implementation of this WISP;
- Regular testing of this WISP's safeguards;
- Ensuring the Company appoints a CISO and that the CISO provides the required annual certifications;
- Evaluating the ability of service providers to comply with the Company's Vendor Risk Policy;
- Reviewing the scope of the security measures in this WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information.

3. Data Security Coordinator Responsibilities

The Data Security Coordinator shall be responsible for:

- Ensuring appropriate data protection provisions are included in our contracts with those services providers including provisions obligating them to comply with the Company's Vendor Risk Policy, 23 NYCRR 500, and other relevant laws and regulations in providing the contracted for services, and obtaining from such service providers written certification that such service provider has a written, comprehensive information security program that is in compliance with Company's Vendor Risk Policy;
- Creating and maintaining a list of PII locations;
- Protecting personal information collected as written or digital data Company-wide by ensuring all employees handling personal identification data are properly trained;
- Educating all data owners, managers, employees and independent contractors, including temporary and contract employees who have access to personal information on the elements of this WISP; and,
- Ensuring Company-wide compliance with this policy and the Company's other policies.

5) Statements of Policy

1. Risk Assessment and Risk Management

The Company shall periodically, but not less than every two (2) years, review and update the Company's Risk Management plan. Such review shall include a reassessment of the risks facing the Company based on updated cybersecurity and other threats.

2. Commitment to Limited Collection of, and Access to, PII

The Company will collect, maintain, and store only that PII which is reasonably necessary to accomplish the legitimate business purpose for which it is collected. The Company shall limit the time PII is retained to what is reasonably necessary to accomplish such purpose, including without limitation to meet any legal or regulatory requirements. The Company shall limit access to PII to those persons who are reasonably required to have access to that PII to accomplish such purpose or to comply with state or federal record retention requirements. All persons granted access to PII shall be informed of this WISP and shall be provided basic training for compliance with this WISP's requirements.

3. Identified Locations of PII

The Company has identified specific electronic databases and servers, along with physical locations, where PII is known to exist. These locations, while not an exhaustive list, are kept by the Data Security Coordinators and are periodically audited by the CISO or the Data Security Manager's representative. It is incumbent upon the Data Security Coordinator to reinforce to the Company's staff and vendors with PII access the importance of preserving the confidentiality of PII.

4. Data Retention

The Company shall, no less frequently than every two (2) years, securely dispose of any Nonpublic Information that is no longer necessary for business operations or for other legitimate business purposes of the Company, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

5. Data Destruction

Destruction of records will be done in a commercially acceptable manner so that PII cannot be practically read or reconstructed, via either a Company-approved shredding service or a cross-cut shredder for paper files or files stored on CD-ROM, DVD, or other such drives. All PII to be shredded by a shredding service must be placed in a properly identified, locked bin and not in an open recycle bin or trash can.

All hard drives from servers or sensitive computer systems designated for replacement or retirement must be erased using software approved of for that purpose by the United States Department of Defense or securely destroyed to render any PII data unreadable and unable to be reconstructed.

Where the Company contracts with a third-party shredding or data destruction company, the Company shall obtain written assurances from the third-party that its disposal practices are in compliance with this WISP and any statutory and regulatory requirements, including without limitation 23 NYCRR 500.

6. Network and Data Segmentation

The Company shall, as appropriate, segment its networks to limit the ability for malware or attackers to move laterally within the organization.

7. Third-party Entrustment

The Company shall take all reasonable steps to verify that any third-party vendor, contractor or service provider with access to PII maintained by the Company has the capacity to protect such PII in a manner consistent with this WISP and the Company's Vendor Risk Policy. To that end, the Company requires representations and warranties from all third-party vendors, contractors and service providers entrusted with PII that they comply with this WISP and/or all relevant legal and regulatory requirements, including those described in 23 NYCRR 500, the California Consumer Privacy Act, and HIPPA. The Company further requires that all such contractors complete, and submit to the Company, a written manifestation of their current and ongoing compliance with this WISP. Should the third-party not provide such documentation, or later withdraw their assent to the requirements, the Company shall no longer provide any PII to said third-party and will take affirmative steps to ensure that previously entrusted PII is destroyed in a manner in-line with that which the Company would use.

8. Termination or Transfer

Employees may leave, be terminated, or change roles within the Company. The relationship between the Company and third parties may change. Where the employee or third party had access to specific PII and the changed relationship negates the need for access, the Company shall take specific affirmative steps to ensure that access to PII is withdrawn.

9. Reporting

Reports described in this WISP shall be created by the party identified in the WISP and in accordance with the WISP.

10. Breaches

Whenever there is a Breach, the Company shall take the following steps:

1) The Company should respond to the Cybersecurity Event in accordance with the Company's Data Breach Incident Response Policy.
2) Where appropriate, a letter of notification of breach shall be sent to the Company's insurance carrier.
3) Where appropriate, a letter shall be sent to the State(s) Attorney General and the Director of Consumer Affairs and Business Regulations or other such entity as required by the laws of the state(s) in which the PII Subject(s) reside(s).
4) Where appropriate, a letter shall be sent by the Company's Data Breach Counsel to the affected PII Subjects notifying them of the breach.
5) An immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in the security practices are required to improve the security of PII.
6) Disciplinary action may be taken against the individual, or individuals, who caused, or contributed to, the breach.

6) Safeguards and Procedures

1. Reporting

The CISO shall report in writing at least annually to the Company's Partner Committee or other such governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to the Company's Data Security Manager or a senior officer of the Company responsible for the Company's cybersecurity program. The CISO shall report on the Company's cybersecurity program and material cybersecurity risks. The CISO's report shall consider to the extent applicable:

(1) the confidentiality of nonpublic information and the integrity and security of the Company's information systems;
(2) the Company's cybersecurity policies and procedures;
(3) material cybersecurity risks to the Company;
(4) overall effectiveness of the Company's cybersecurity program; and
(5) material cybersecurity events involving the Company during the time period addressed by the report.

2. Third-party Validation

The Company's Data Security Manager shall engage an outside entity to periodically, but not less than every two years, to assess the Company's compliance with this WISP, legal and regulatory requirements identified by the Company, and industry standards and best practices which the Company feels are most relevant to its work. By way of example, without limitation, the Company's current WISP is based on the U.S. National Institute for Standards and Technology Cybersecurity Framework, the Center for Internet Security's Basic 6 Controls, 23 NYCRR 500, and the California Consumer Privacy Act, among other requirements.

3. Penetration Testing and Vulnerability Scanning

The Company shall periodically engage a third-party to provide:

(1) annual penetration testing of the Company's Information Systems determined each given year based on relevant identified risks in accordance with the Company's Risk Management Policy; and
(2) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Company's Information Systems based on the Company's Risk Management Policy.

4. Logging and Auditing

The Company's Information Systems shall be configured to, to the extent applicable and based on the Company's Risk Management Policy, include audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the Company. The Company shall maintain records required by this section for **not fewer than three years**.

5. Network Design Considerations

The Company shall maintain its firewall and intrusion detection/prevention systems so that networks with data servers can be isolated from end user systems.

6. Firewall

A commercial-grade firewall shall be maintained at the Company protecting systems containing PII from both external and internal unauthorized access. The software running on the firewall shall be reasonably current.

7. IPS

The Company has as part of its Firewall an Intrusion Prevention System that monitors traffic across its network to help mitigate against unauthorized access. The software shall be kept reasonably current.

8. VPN

The Company shall maintain a Virtual Private Network ("VPN"), which will necessarily be used to encrypt data connections to the Company where there is a reasonably foreseeable possibility that PII will be carried over the connection and an SSL HTTP connection is not feasible.

9. System Hardening and Security Patches of Company-Controlled Systems

The Company's Information Systems will be security hardened with current security configurations and removal of any default credentials. Reasonable means and methods shall be taken to ensure that security-related critical patches are applied to operating systems and application software. All available patches will be reviewed and approved/rejected within thirty (30) days of their release, and all approved patches will be deployed within the Company not later than sixty (60) days after the patches were released.

10. Anti-Virus and Malware:

There shall be reasonably up-to-date versions of virus/malware protective agents running on Company-owned computers, which report to a central server that is reviewed regularly for compliance with policy.

11. Data Flow

The CISO shall create a data flow diagram that illustrates how different types of data flow into, within, and out of the Company. This data flow diagram shall define the different categories of entities with whom the Company routinely exchanges information (e.g., external service providers (e.g., physicians, investigators, etc.), customers, cloud service providers, etc.) the types of data exchanged with each entity type (e.g., names, addresses, social security numbers, etc.), and the location(s) where those entities operate (e.g., US only, Europe, China, etc.). This data flow diagram be used to inform anomaly detection and data loss prevention.

12. Network Segmentation

The CISO shall implement network segmentation as appropriate within the organization. The network segmentation will compartmentalize the equipment in the organization based on the equipment's business function and shall be designed to prevent lateral movement of malware or attackers throughout the organization.

13. Network Monitoring

The CISO shall establish tools for monitoring network traffic to identify anomalous behavior. Such tools shall collect and analyze information from sources including, without limitation, audit logs from network equipment. Anomalies shall be promptly reported by the CISO to appropriate persons within the Company or in a third-party service provider to be addressed promptly. The CISO shall maintain a list of the anomalies detected, including the date and time of the detection. Such list shall also describe the severity of the issue, the steps taken to address the anomaly (e.g., false alarm and no actions taken, shut down network port, etc.) and the time at which the step(s) were initiated and completed.

14. Identity Management

The Company will maintain a procedure for managing computer accounts for active employees to ensure that each active employee has his or her own unique computer account(s). The Company recognizes that accurate forensics is only possible where a single user has access to a specific computer account, and will take business-reasonable steps to ensure that employees do not share account login information except in emergencies or where appropriate consistent with the Company's Risk Management Policy. The Company shall promptly disable accounts of those individuals who are no longer employed and/or entrusted by the Company.

15. Access Control

Access to PII shall be electronically limited to those employees or other authorized users with unique usernames. The Company shall further limit access to its Information Systems, and the nonpublic information contained therein, based on the principle of Least Privilege. The CISO shall, no less frequently than every six months, review the access privileges for each user and system account to ensure they are consistent with this policy. All accounts

assigned to Company employees who resign, or whose employment by the Company is otherwise terminated, shall be disabled as soon as practical after the employee's employment terminates.

16. Privileged Accounts

The CISO shall ensure that only specific, authorized individuals in the Company are granted accounts with administrator or other privileged access rights. This includes, without limitation, preventing employees from having "local admin" accounts on their individual computers. Where consistent with the Company's business practices, the CISO shall also ensure that all users with privileged accounts also have secondary, nonprivileged accounts which are used to conduct their day-to-day operations for the Company. The CISO shall also ensure that separate service accounts are created for each service that needs such an account, and that unique passwords are used for each service and user account. The CISO shall also ensure that any electronic copies of privileged account passwords or other credentials, including without limitation private encryption keys or related information, are stored in encrypted files where possible.

17. Passwords

The Company requires unique usernames and passwords for any individual or resource accessing any system that may contain PII. Passwords must meet minimum requirement described by the United States National Institute for Standards and Technology (NIST) in Special Publication 800-63B Section 5.1. NIST SP 800-63B currently requires a minimum password length of eight (8) characters, and that the Company not require, but should permit, the use of mixed cases (i.e., upper and lower case), numerals, and special characters in passwords. NIST SP 800-63B also requires that all passwords be checked against a common password dictionary and that users be required to select a different password if their password, or a common variation of the password, is in the dictionary. In addition:

- Accounts shall be locked after ten (10) unsuccessful login attempts.
- Enforcement of this password policy shall be maintained through electronic means.
- Usernames and passwords shall not be shared amongst individuals.
- Vendor-assigned and default passwords shall be changed promptly and **must** be changed before the system accessed through said password contains or can access any PII.

18. Multifactor Authentication

Based on its Risk Management Program, the Company shall use effective controls, which may include multi-factor authentication or risk-based authentication, to protect against unauthorized access to nonpublic information or information systems. Multi-factor authentication shall be utilized for any individual accessing the Company's internal networks from an external network, unless the CISO has approved in writing the use of reasonably equivalent or more secure access controls.

19. Electronic File Storage

The Company shall maintain a file server or other secure means of data storage of sufficient speed and storage capacity to hold any and all electronic documents that may contain PII. No PII should be stored on individual desktop/ laptop computers. All data must comply with the Company's Data Classification and Usage Policy.

20. Encryption of Data at Rest

Nonpublic Information shall be encrypted whenever such information is stored (i.e., at "rest"). To the extent the CISO determines that encryption of nonpublic information at rest is not feasible, the Company may instead secure such nonpublic information using effective alternative compensating controls reviewed and approved by the CISO. All such exceptions shall be documented and included in the CISO's annual report.

21. Encryption of Removable/Portable Media

Where electronic files containing PII must unavoidably be taken from an approved storage location and placed on portable media (including, but not limited to, a computer's internal hard drives, USB "thumb drives," externally connected drives and other removable media), the files containing PII must comply with the standards set in the Company's Data Classification and Usage Policy.

22. Encryption of Data in Transit/Motion

Where feasible, when Nonpublic Information is transmitted over a data network where data interception is reasonably foreseeable, Nonpublic Information will be encrypted using the Company approved encryption. The Company shall maintain SSL Certificates, managed by a trusted root host, which shall be used on web pages served by the Company over which there exists the reasonably foreseeable possibility that Nonpublic Information may be accessed. To the extent the CISO determines that encryption of nonpublic information in transit over external networks is infeasible, the Company may instead secure such nonpublic information using effective alternative compensating controls reviewed and approved by the CISO. All such exceptions shall be documented and included in the CISO's annual report.

23. Backups

All business-critical information shall be replicated between the Company's data centers to ensure availability. All data shall be backed up no less frequently than on a weekly basis. Wherever feasible, server backups shall be encrypted using an industry-accepted data encryption standard. Backups shall be tested at least annually to ensure that at least a randomly-selected subset of the information is able to be restored.

24. Data Monitoring

To the extent possible, the Company shall monitor information moving within and outside the Company's networks for data loss prevention purposes.

25. Data Security Training and Acceptable Use:

All new employees shall receive training on Information System security, acceptable use of the Company's computer equipment, and related issues. The Company shall maintain an information security employee training program. Employees whose positions at the Company require contact with PII shall be provided additional training, within their departments, commensurate with the potential exposure. The Company will maintain an acceptable use policy with which all persons granted access to the Company's network will be required to comply.

26. Physical Security

(1) Filing Cabinets: Where filing cabinets are to be used for the storage of PII, the filing cabinets are to remain locked unless the need to access the files within is imminent or current. Should removal of files containing PII from a filing cabinet be necessary, the files themselves must be protected against unauthorized access and if the files will not be returned to the filing cabinet promptly, the filing cabinet shall be locked. Files must be returned to filing cabinets, which are then to be locked, no later than the end of the workday of the employee that removed them, unless their overnight storage outside their designated filing cabinet is approved, in writing, by the appropriate Data Security Coordinator.

(2) Transport: All efforts will be made to minimize the physical transport of printed PII, substituting encrypted electronic data transport instead. Where printed PII must be transported, the carrier shall either be commercial and bonded, or a trained member of the Company community.

(3) Server storage: All servers or other computing equipment shall be stored in locked rooms/closets and only those with a need to access such rooms/closets shall be granted access thereto.

27. Employee and Contractor/Vendor Terminations

All records containing PII, in any form, must be returned at the time of termination of the relationship. If return is not feasible, destruction in accordance with industry standards, along with proof of such destruction, is acceptable.

At the time of termination of the relationship, all electronic and physical access to PII must immediately cease and be blocked. Former employees and third parties must return keys, IDs (if not required for other legitimate purposes), access control tokens and cards. Electronic locks access shall be disabled. Continued access to PII by former employees and third parties with whom the business relationship has been terminated must be expressly authorized, in writing, by the Data Security Manager.

28. Asset Inventory

The Company shall maintain an accurate inventory of the devices in its Information Systems environment, including an inventory of all software installed on those devices. The inventory shall be maintained automatically, and the software used to perform the inventory shall alert the CISO to all changes to the environment, including, without limitation, any unauthorized new devices or unauthorized software discovered on the devices. The CISO shall, no less frequently than every six (6) months, review, and certify that, the asset inventory:

(1) is accurate;
(2) that devices and software which are no longer receiving support or other updates from the vendor have either been removed from the Information Systems environment or appropriately quarantined to reduce risk to the Company consistent with the Company's Risk Management Plan; and,
(3) that only approved software and hardware exist in the Information Systems environment.

29. Device Management

The Company shall establish standard device operating system and application images containing the tools needed by the majority of the Company's employees. All other software installed in the environment must be approved by the CISO and must be recorded in the Asset Inventory. The Company shall implement policies which permit the Company to remotely manage any devices containing Company content, including employee mobile devices. Such remote management shall permit the Company to:

(1) ensure all devices have encryption enabled by default for all data stored therein; and
(2) where possible, to permit the Company to securely wipe the devices of any Company data, including without limitation data from Company clients, under circumstances approved by the Data Security Manager. Such circumstances may include, without limitation, employee termination or severance from the Company, and the loss or theft of a device containing Company information.

30. Maintenance

All maintenance and repair of the Company's Information System shall be logged and shall only be performed with tools approved by the CISO. Any remote maintenance shall be logged and performed in a manner that prevents unauthorized access to the Company's Information System.

31. Business Continuity and Disaster Recovery Planning

The Company shall establish and maintain a Business Continuity and Disaster Recovery plan that is consistent with the Company's Risk Management program.

32. Systems and Application Development and Quality Assurance

The Company does not currently use any custom or in-house developed applications. In the event the Company begins using such applications, the Company shall create written procedures, guidelines and standards designed to

ensure the use of secure development practices for such applications and procedures for evaluating, assessing, or testing the security of externally developed custom applications. All such procedures, guidelines and standards shall be periodically reviewed, assessed, and updated as necessary by the CISO (or a qualified designee) of the Company.

7) Enforcement

Any person that violates any of the measures found in this plan will be subject to the same disciplinary actions outlined in the Company's Confidentiality Agreement for employees, or the Acceptable Usage Policy and Code of Conduct for students.

8) Cross-references to Related Policies and Plans

Data Classification and Usage Policy

Records Retention and Destruction Policy

Data Classification and Use Policy

Risk Management Policy

Vendor Risk Policy

Data Breach Incident Response Plan

Business Continuity and Disaster Recovery Plan

9) Approval and Revisions

Date	Name	Revision(s)
14-JUN-2021	J. Goepel	Updated to clarify backup policies.
31-DEC-2020	J. Goepel	Updated based on changes in the environment.
12-NOV-2020	J. Goepel	Updated to reflect changes in different Policies and Plans.
05-OCT-2020	J. Goepel	Document created to memorialize ad hoc and unwritten policies already existing within the Company.