Effective May 3, 2023. This Written Information Security Policy supersedes and replaces all prior versions.

Written Information Security Policy

POLICY STATEMENT

State and Federal Laws provide standards for protecting the security and confidentiality of non-public customer personal information collected or maintained by or on behalf of businesses. Provider established an Information Security Program (the "Program") to assure compliance with applicable laws. As required by law, the Program provides for the security and confidentiality of personal identifying information or sensitive personal information collected, protects against anticipated threats or hazards to the security or integrity of such information, and protects against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any of our customers.

It is the policy of Provider to comply, and to require its employees to comply, with all applicable federal, state, and local laws and regulations, as well as Provider's policies and procedures, governing information security, confidentiality, and privacy. The Program is universally applicable to all services offered by Provider and addresses the security and confidentiality of business records containing personal identifying information or sensitive personal information as those terms may be defined by applicable law (collectively, "Information").

RESPONSIBLE PARTY FOR INFORMATION SECURITY PROGRAM

Provider will designate an Information Security Program Coordinator ("Coordinator") who will be primarily responsible for coordinating and overseeing the Program. The Coordinator will report to the Chief Executive Officer.

RISK ASSESSMENT AND SAFEGUARDS

Because there is an inherent risk in handling and storing customer information, Provider will routinely monitor its operations related to the handling of the Information. Such monitoring is designed to protect customers from wrongful use or disclosure of their private information and protect the company from potential liability.

Provider will take steps to identify and assess internal and external risks to the security, confidentiality, and integrity of Information that could result in the unauthorized access, disclosure, misuse, alteration, destruction or other compromise of such Information. The risk assessment will be conducted by personnel or counsel with sufficient expertise, and should (at a minimum) include consideration of any risks, current safeguards to manage those risks, and an analysis of Information protection in each relevant aspect of Provider's operations, including:

- Employee training and management policies for controlling access and use of such Information;
- Information systems (including network and software design, as well as Information processing, storage, transmission and disposal for both paper and electronic records); and

- Detecting, preventing and responding to attacks, intrusions, or other system failures (including data processing and telephone communication), as well as contingency planning and business continuity.

The Coordinator will establish procedures for identifying and assessing risks in each relevant area of Provider's operations outlined above. The Coordinator will be responsible for ensuring that company staff is trained in the relevant legal requirements for handling and storing Information. The Coordinator will be responsible for maintaining a high level of awareness and sensitivity to safeguarding Information within all departments.

IMPLEMENTING SAFEGUARDS

The Coordinator will design, implement, and maintain in writing, the administrative, technical, and physical safeguards necessary to control the risks identified through risk assessment, and will regularly monitor the effectiveness of such safeguards. Safeguards are to be designed and implemented in accordance with the nature and scope of company activities and the sensitivity of the Information at issue. Safeguards are to include:

Administrative Safeguards

- Security management process. Policies and procedures to prevent, detect, contain, and correct security violations. This safeguard will be implemented by:
    - An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Information.
    - Security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
    - Appropriate sanctions against workforce members who fail to comply with security policies and procedures.
    - Procedures to regularly review records of Information system activity, such as audit logs, access reports, and security incident tracking reports.
- Workforce security. Policies and procedures to ensure that all company employees have appropriate access to electronic Information and to prevent any unauthorized company employees from obtaining access to electronic Information. This safeguard may be implemented by one or all of the following, as appropriate:
    - Procedures for the authorization and/or supervision of company employees who work with electronic Information or in locations where it might be accessed;
    - Procedures to determine that the access of a company employee to electronic Information is appropriate.
    - Procedures for terminating access to electronic Information under appropriate circumstances, such as, for example, when the employment of a company employee ends.
- Information access management. Policies and procedures for authorizing access to electronic Information that are consistent with applicable law and best practices related to information security. This safeguard may be implemented by one or all of the following, as appropriate:
    - Policies and procedures for granting access to electronic Information, for example, through access to a workstation, transaction, program, process, or other mechanism.\

    - Policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
- Security awareness and training. A security awareness and training program for all company employees (including management). This safeguard may be implemented by establishment of periodic security updates, procedures for guarding against, detecting, and reporting malicious software, procedures for monitoring log-in attempts and reporting discrepancies, and/or procedures for creating, changing, and safeguarding passwords.
- Security incident procedures. Policies and procedures to address security incidents. This safeguard will be implemented by identification and response to suspected or known security incidents; mitigation, to the extent practicable, of any harmful effects of security incidents that are known to the company; and documentation of security incidents and their outcomes.
- Contingency plan. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic Information. This safeguard will be implemented by
    - Procedures to create and maintain retrievable exact copies of electronic Information.
    - Procedures to restore any loss of data.
    - Procedures to enable continuation of critical business processes for protection of the security of electronic Information while operating in emergency mode;
    - In addition, this safeguard may be implemented by one or all of the following, as appropriate:
        - Procedures for periodic testing and revision of contingency plans.
        - Assessment of the relative criticality of specific applications and data in support of other contingency plan components.
- Evaluation. Performance of periodic technical and nontechnical evaluations in response to any environmental or operational changes affecting the security of electronic Information, that establishes the extent to which the company's security policies and procedures continue to meet the requirements of applicable law or otherwise remain effective.

Physical Safeguards

- Facility access controls. Policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. This safeguard may be implemented by one or all of the following, as appropriate:
    - Procedures that allow facility access in support of restoration of lost data under any disaster recovery plan or emergency mode operations plan in the event of an emergency.
    - Policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
    - Procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
    - Policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

- Workstation use. Policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic Information.
- Workstation security. Physical safeguards for all workstations that access electronic Information, to restrict access to authorized users.
- Device and media controls. Policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic Information into and out of a facility, and the movement of these items within the facility. This safeguard will be implemented by:
    - Policies and procedures to address the final disposition of electronic Information, and/or the hardware or electronic media on which it is stored.
    - Procedures for removal of electronic Information from electronic media before the media are made available for re-use.
    - In addition, this safeguard may be implemented by one or all of the following, as appropriate:
        - A record of the movements of hardware and electronic media and any person responsible therefor.
        - A retrievable, exact copy of electronic Information, when needed, before movement of equipment.

Technical Safeguards

- Access control. Technical policies and procedures for electronic information systems that maintain electronic Information to allow access only to those persons or software programs that have been granted appropriate access rights. This safeguard will be implemented by:
    - A unique name and/or number for identifying and tracking user identity.
    - Procedures for obtaining necessary electronic Information during an emergency.
    - In addition, this safeguard may be implemented by one or all of the following, as appropriate:
        - Electronic procedures that terminate an electronic session after a predetermined time of inactivity.
        - A mechanism to encrypt and decrypt electronic Information.
- Audit controls. Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic Information.
- Integrity. Policies and procedures to protect electronic Information from improper alteration or destruction. This safeguard may be implemented by electronic mechanisms to corroborate that electronic Information has not been altered or destroyed in an unauthorized manner.
- Person or entity authentication. Procedures to verify that a person or entity seeking access to electronic Information is the one claimed.
- Transmission security. Technical security measures to guard against unauthorized access to electronic Information that is being transmitted over an electronic communications network. This safeguard may be implemented by one or all of the following, as appropriate:
    - Security measures to ensure that electronically transmitted electronic Information is not improperly modified without detection until disposed of.
    - A mechanism to encrypt electronic Information whenever deemed appropriate.

The Coordinator will prepare and maintain written safeguards and will provide guidance on implementation of safeguards to all affected company employees.

CYBER ATTACK SAFEGUARDS

To minimize the risks associated with cyber attacks, the Coordinator will perform the following risk-mitigation tasks:

- Identify systems without which it would be difficult for the business to operate.
- Establish a policy regarding transferring funds.
- Require verbal verification of all new account numbers and any previously verified account number that has changed for any reason.
- Train any employees that have the ability to transfer funds on behalf of the business to follow the policy according to these procedures.
- Implement multi-factor authentication
- Ensure that patches are current.
- Implement a system where backups are reliable, current, and independent from the primary network.
- Upgrade any unsupported operating systems for desktops and servers.
- Scan and filter incoming emails and files that could contain viruses.
- Secure or disable All remote desktop endpoints
- Encrypt all sensitive and confidential information.
- Restrict network administrative privileges. Computer networks rely on a hierarchical system of access levels to help protect critical parts of the network from both accidental and intentional alterations.

PERIODIC EVALUATION AND REVISION OF THE PLAN

This Program will be reviewed and adjusted periodically. The Coordinator will review the Program annually to ensure ongoing compliance, as well as consistency with other existing and future laws and regulations. The Coordinator will provide periodic reports on the status of the Program and note any changes to the overall risk assessment and changes to established safeguards. Some areas of the company may require more frequent review than others, such as IT, records management, or any other area that comes in contact with a high volume of Information or is especially vulnerable to technological or procedural risks and threats.

RISK ASSESSMENT PROCESS

Provider is legally required to safeguard its clients' Information. Each department is responsible for maintaining an active risk assessment policy. The Risk Assessment Process identifies various events or threats within the department that could negatively affect the institution strategically or operationally. Management should evaluate the likelihood of various events and rank the possible impact. Assessed risks can fall under a number of different categories, including:

- Security breaches - Security breaches include external and internal security breaches, programming fraud, computer viruses, hacking, or denial of service attacks.
- System failures - System failures include network failure, interdependency risk, interface failure, hardware failure, software failure, or internal telecommunication failure.

- External events - External events include weather-related events, earthquakes, terrorism, cyber-attacks, inoperable or disabled utility lines or widespread power outages that cause system or facility failures.
- Systems development and implementation problems - System development and implementation problems include inadequate project management, cost/time overruns, internal or external programming errors, failure to integrate and/or migrate successfully from existing systems, or failure of the systems to meet business requirements.
- Improper Disposal Procedures – Improper disposal procedures may allow a third party to steal or access data, reconstruct data, or commit 'dumpster diving.'

For example, if Information is stored on a particular computer, the department's risk assessment procedure must include an analysis of that computer. The analysis would include a discussion of whether the Information is accessible to anyone who has physical or network access to the computer, whether there were safeguards such as login and password access or firewall software, and an assessment of the potential risk associated with unauthorized access. The department would then be responsible for implementing safeguards to mitigate the assessed risk. Installation of firewalls, restricted access, data encryption, or limited network/internet access are all possible safeguards in this example. The department has discretion to decide whether a proposed safeguard or safeguards constitutes an adequate remedy for an assessed risk.

All risk assessments must identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such Information. The assessment must also address the sufficiency of any safeguards in place to control these risks. The assessment, at a minimum, must include employee training and management, information systems (including network and software design, as well as information processing, storage, transmission and disposal), and detecting, preventing, and responding to attacks.

PROPOSED TECHNICAL SAFEGUARDS

All Provider departments must employ technical safeguards to ensure that electronically stored Information is secure from unauthorized access or use. This section includes a number of possible safeguards that may be used, but is not an all-inclusive list of ways to safeguard Information. The Coordinator will ultimately evaluate and employ technical safeguards as he or she deems appropriate.

System / Security Updates: Computers should have the most recently available and appropriate software security patches, commensurate with the identified level of acceptable risk. For example, installations that allow unrestricted access to resources must be configured with extra care to minimize security risks. Special attention must be given to security-related software such as anti-virus and firewall protection to ensure that they provide the maximum level of protection. This applies not only to large systems but also to smaller computers which, if compromised, could constitute a threat to the security, confidentiality or integrity of Information.

Access Authentication: Adequate authentication and authorization functions must be provided, commensurate with appropriate use and the acceptable level of risk. For example, access to Information may be restricted through the use of login and password protection. For higher levels of risk, additional safeguards such as use of encryption technologies may be employed.

Passwords must be unknown, unrecorded, and unrecoverable by system administrators or system support staff. The result is that users cannot request their old password if they forget, and must set a new password after their identity has been confirmed. All passwords must be at least 6 characters long and contain at least one letter and one number. Users will be required to change their password at least every 90 days. Single use temporary passwords may be issued when the situation permits.

Login Security Measures: There must be a limit to the number of repeated unsuccessful attempts to log into an application or server that deals with Information. For example, a system that “locks” access from a particular account after 3 failed attempts would meet this criterion. The ability to restore access to “locked” accounts should be restricted to the appropriate IT administrator.

Secure Transmissions: Encryption of data should be considered for instances involving the transportation of data across any network, particularly for any communications that connect to an outside system or network (such as the Internet). Users should clearly understand that normal email cannot be considered a secure way to transport Information, particularly outside of the local email server. Versions of email that encrypt the messages and attachments can be obtained and should be used wherever large amounts of Information are involved.

Remote Access: Employees and authorized third parties (customers, vendors, etc.) can use dial-in connections, remote desktop connections or other internet-based access connections to gain access to the corporate network. Remote access should be strictly controlled, using one-time password authentication.

It is the responsibility of employees with remote access privileges to ensure a remote access connection to Provider is not used by non-employees to gain access to company information system resources. An employee who is granted remote access privileges must remain constantly aware that remote access connections between their location and Provider are literal extensions of Provider's corporate network, and that they provide a potential path to the company’s most sensitive Information. The employee and/or authorized third party individual must take every reasonable precaution to protect the Information of Provider and its customers.

Analog and non-GSM digital cellular phones cannot be used to connect to Provider's corporate network, as their signals can be readily scanned and/or hijacked by unauthorized individuals. Only GSM standard digital cellular phones are considered secure enough for connection to Provider's network.

Note: Remote access accounts are considered “as needed” accounts. Account activity should be monitored, and if a remote access account is not used for a period of six months the account should be eliminated and no longer function. If remote access is subsequently required, the individual must request a new account as described above.

Access Privileges: Each department shall confirm that employee tasks require access to Information before allowing access. Employees shall only have access to Information necessary to complete their job functions – no “blanket” access will be given to all Information unless deemed necessary. All employees who have access to Information will be required to sign a confidentiality agreement.
Software Installations: The IT department should ensure that only required products are enabled on a computer that has access to Information, and require IT approval and supervision for

software installs to reduce the risk of introducing a security risk via an installed program (such as an imbedded virus or Trojan).

Employee Training: All employees that have access to Information or work with systems that handle Information should receive adequate training for handling and disposal of such Information.

EMPLOYEE GUIDE ON PROPER HANDLING OF INFORMATION

General Use and Ownership

1. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet / Intranet / Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
2. Provider recommends that any information that users consider sensitive or vulnerable be encrypted.
3. For security and network maintenance purposes, authorized individuals within Provider may monitor equipment, systems and network traffic at any time.
4. Provider reserves the right to audit networks and systems on a periodic basis to ensure compliance and security.

Security and Proprietary Information

1. The user interface for information contained on Internet / Intranet / Extranet-related systems should be classified as either confidential or not confidential, as defined by Provider confidentiality guidelines. Examples of confidential information include but are not limited to: nonpublic personal customer information (such as names, addresses, social security number, etc.), corporate strategies, competitor sensitive information, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Both system and user level passwords should be changed at least every 90 days.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (typically, [Ctrl]+[Alt]+[Del] followed by [Space] for Windows users) when the host will be unattended.
4. All hosts used by the employee that are connected to the Provider Internet/Intranet/Extranet, whether owned by the employee or Provider, shall be continually executing approved virus-scanning software with a current virus database, unless overridden by departmental or group policy.
5. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
6. Employees will report any suspected infections of viruses, e-mail bombs, or Trojan horse code to the appropriate IT representative for immediate corrective action.

Loss of Company-Owned Devices

Provider employees who possess company-owned laptop computers or other portable electronic devices are expected to secure them whenever they are left unattended. Without limitation, employees shall not leave any company-owned devices in a motor vehicle, regardless of whether that vehicle is locked, unless the vehicle is parked in a secure, access-controlled parking facility located either at Provider's business premises or at the employee's home (e.g., an attached garage at a single-family residence).

In the event a company-owned or controlled laptop computer or other device is lost, stolen or damaged, the loss, theft or damage must be reported immediately to the employee's immediate supervisor and to Provider's IT department.

If Provider determines that a company-owned laptop computer or other portable electronic device in an employee's possession was lost or damaged either in violation of this policy or under circumstances indicating that the employee was negligent, Provider may deduct the costs of the lost, stolen or damaged device from the employee's paycheck.

Personally Owned Devices

Authorized employees and third parties may wish to use their Personally Owned Devices (PODs) for work purposes, for example making and receiving work phone calls and text messages on their own personal cellphones, using their own tablet computers to access, read and respond to work emails, or working in a home-office.

Bring Your Own Device (BYOD) is associated with a number of information security risks such as:

- Loss, disclosure or corruption of corporate data on PODs;
- Incidents involving threats to, or compromise of, the corporate ICT infrastructure and other information assets (e.g., malware infection or hacking);
- Noncompliance with applicable laws, regulations and obligations (e.g., privacy or piracy);
- Intellectual property rights for corporate information created, stored, processed or communicated on PODs in the course of work for the organization.

Individuals who wish to opt-in to BYOD must be authorized by management and must explicitly accept the requirements laid out in this policy. Provider may choose not to authorize individuals, or to withdraw the authorization, if they deem BYOD not to be appropriate and in the best interests of the company. Provider will continue to provide its choice of fully owned and managed ICT devices as necessary for work purposes, so there is no compulsion for anyone to opt-in to BYOD if they choose not to participate.

The BYOD requirements are as follows:

1. PODs must use appropriate forms of device authentication approved by Provider's IT department, such as digital certificates created for each specific device. Digital certificates must not be copied to or transferred between PODs.
2. BYOD users must use appropriate forms of user authentication approved by Provider's IT department, such as user IDs, passwords and authentication devices.
3. Provider may backup, retrieve, modify, determine access and/or delete corporate data without reference to the owner or user of a POD.
4. Provider may seize and forensically examine any POD believed to contain, or to have contained, corporate data where necessary for investigatory or control purposes.

5. Suitable antivirus software must be properly installed and running on all PODs.
6. Any POD used to access, store or process sensitive information must encrypt data transferred over the network and while stored on the POD.
7. While employees have a reasonable expectation of privacy over their personal information on their own equipment, Provider's right to control its data and manage PODs may occasionally result in support personnel unintentionally gaining access to employees' personal information. To reduce the possibility of such disclosure, POD users are advised to keep their personal data separate from business data on the POD in separate directories, clearly named (e.g. "Private" and "BYOD").
8. Employees shall take care not to infringe other people's privacy rights. For example, without limitation, employees shall not use PODs to make audio-visual recordings at work.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Provider authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Provider-owned resources.

The lists below are by no means exhaustive, but are included to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

1. Transmitting, sharing or otherwise exposing confidential client information with any outside party or unauthorized Provider employee.
2. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
5. Port scanning or security scanning is expressly prohibited unless prior notification to Provider is made.
6. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
7. Circumventing user authentication or security of any host, network or account.
8. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
9. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

10. Providing information about, or lists of, Provider employees to parties outside Provider
11. Disposing of business records containing personal identifying information or sensitive personal information without first destroying or arranging for the destruction of those records by shredding, erasing, or otherwise modifying the personal identifying information or sensitive personal information in those records to make the information unreadable or undecipherable.

Recommended processes to prevent virus problems:

- Always run the only the most current Provider recommended anti-virus software.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then “double delete” them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is a business requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.