Updated: 2022-02-03

ENOVAPOINTS SECURITY CONTROLS

1. Information Security Controls, Risk Assessment and Treatment

EnovaPoint performs a Risk Assessment periodically and upon significant organizational, information technology, or other relevant changes. EnovaPoint documents results of the Risk Assessment. EnovaPoint documents and implements a plan of risk mitigation measures based on the results of the Risk Assessment.

2. Management Direction for Information Security

2.1. Information Security Policy. The EnovaPoint's top management has approved an Information security management system (ISMS) policy. The information security policy applies to all employees to maintain the security of the organization's information. To ensure the consistency and relevance, adequacy and effectiveness of the policy is reviewed periodically (at least once a year).

EnovaPoint's information security policy is (a) comprehensive, addressing the information security risks and controls identified through the Risk Assessment process, for each area of information security (i.e., user access, system development and change, business continuity, etc.) (implemented supplemental policies); (b) reflects the requirements of applicable law, including Data Protection laws; (c) approved by management; (d) published and communicated to all employees and third-party contractors (if applicable); and (e) periodically reviewed and updated (at least once a year).

2.2. Personnel Confidentiality Obligations. EnovaPoint management requires employees and third-party contractors with access to Customer Data to commit to written information security, confidentiality, and privacy responsibilities with respect to that information. These responsibilities must be binding and shall survive termination or change of employment or engagement. Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Customer Data.

3. Personnel management

3.1. Background Check. The history of all job applicants must be validated without prejudice to applicable laws, regulations and ethics, and in compliance with operational and information requirements. All job applicants must be of impeccable reputation, have no complaints regarding the leakage of information, disclosure of know-how, etc.

3.2. Information Security Training. All employees of the organization must be trained and kept informed of changes in the organization's policies and procedures related to their work.

4. Access Control

4.1. Access Control policy. EnovaPoint adheres to the principle of least privilege, specifying that users of EnovaPoint systems will be given access to only the information and resources necessary to perform their job functions as determined by Senior Management. The system privileges granted to every user must be reevaluated quarterly to determine whether currently-enabled system privileges are needed to perform the user's current job duties. Inappropriate access shall be revoked immediately upon identification.

4.2. Password Management Policy define management of user passwords including appropriate use, expiration, and modification of passwords used to access EnovaPoint's and third-party vendor operating systems, applications, and data. EnovaPoint shall institute a strong password policy and procedure to help ensure the protection and privacy of covered data at rest or in transit. A strong password configuration policy shall be enforced on all systems that provide for the implementation of passphrases and determine the necessary length, complexity, and expiration of system passwords.

4.3. Network and network service access management. Restricted access to Customer Data can only be accessed through an office VPN. Employee's devices are encrypted and controlled remotely. Firewall, IDS / IPS, intrusion detection system, instruction prevention and Azure Sentinel are used for enterprise network security.

5. Physical Security.

The office premises are protected by an alarm system. Each employee has their own office access code. The internal server room is a separate and has separate alarm system. Other persons enter office only with the admission of the employees of the organization. No sensitive Customer Data are stored or processed on EnovaPoint's premises.

6. Protection of Equipment.

6.1. Equipment storing or processing Customer Data shall be located within a dedicated, secured, and isolated facility (e.g., data center). Any data stored, while at rest, shall be stored using an encryption method appropriate for the medium of storage. The following encryption methods are in place for stored confidential data (Customer Data is defined as confidential):

- Microsoft SQL Server - Transparent Data Encryption (TDE) (AES-256 algorithm)
- Virtual Machines - Azure Disk Encryption (AES-256)
- Azure Storage - Azure Storage encryption (AES-256)
- Office 365 (internal documents) - secured both at rest (BitLocker, DKM) and in transit (TLS) with end-to-end encryption.

- Workstations – BitLocker

6.2. EnovaPoint shall implement controls to protect equipment, information, and assets located off-premises and/or during remote access sessions such as teleworking or remote administration. Teleworking, Electronic Communication, Network Protection policies and IT Security Rules are implemented and enforced.

6.3. The equipment used by the employees of the company in their activities is accessible only with the granted rights and only with a password. Users must use own login keys to use specialized software.

6.4. Users shall protect unattended sessions and equipment. When users do not use the computer for more than 5 minutes, the computer must be locked. When users do not use the computer for more than 10 minutes, the computer locks automatically. Users working remotely must ensure protection against any access by third parties to the information. Users must always turn on screen savers with an activated screen when leave the computer. Additionally, a clear desk and clear screen policy is enforced.

7. Asset Management.

7.1. Asset Register. All assets in the organization are inventoried. EnovaPoint will inventory and track all assets, physical and digital, that are used to view or store confidential information annually. The asset inventory will include all systems connected to the network and network devices themselves. Examples of items to be inventoried could be desktop workstations, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, telephony, etc.

7.2. Use of Assets. Employees and third-party contractors (if applicable) shall agree to documented policies for the acceptable use and handling of assets. Assets shall be returned immediately upon termination of employment/contact and return of assets shall be tracked and verified.

7.3. System Hardening. EnovaPoint has implemented formal, documented system hardening procedures and baseline configurations. Unsupported software or hardware shall not be used.

8. Communications Security

8.1. Network Security. EnovaPoint shall segregate network systems containing Customer Data from network systems supporting internal or other activity. EnovaPoint shall logically

segregate Customer Data within a shared service environment. EnovaPoint shall secure network segments from external entry points where Customer Data is accessible.

8.2. EnovaPoint shall implement a secure gateway (firewall) to protect and segregate the internal EnovaPoint network from external networks or DMZs. The selected gateway shall conform to industry standards and be capable of enforcing the security policies defined in the Access Control Policy.

8.3. Remote connections. All remote connections to the Customer Data network shall be done using a secured VPN connection. A multi-factor authentication method shall be implemented to provide added security for remote connections. Provisioning of users for remote access shall adhere to the Access Control and Teleworking policies. Prior to enabling hardware tokens for remote access, the assigned user's identity must be verified in person.

9. Cryptographic Controls.

1.1. Encryption. Customer Data, including personal data, shall be encrypted at rest and in transit.

1.2. Key Management. Encryption keys must be protected such that only authorized users and applications can access the keys. The keys used to encrypt data should not be stored on the same media as that data. Whenever keys are stored either physically or logically in close proximity to the data that it is protecting mitigating controls must be in place to ensure a compromise of the data does not happen. Such mitigating controls must include, but are not limited to, the encryption of the keys themselves.

10. Penetration Testing

EnovaPoint shall perform annual penetration testing for systems and applications that store or allow access to Customer Data, including personal data, or when significant changes are made to those systems and applications. Upon request by Customer, EnovaPoint shall provide latest penetration test report with results.

11. Vulnerability Management

EnovaPoint shall install, maintain, and protect the corporate network using industry standard best practices including, but not limited to, a network firewall, an intrusion detection or prevention system, and anti-virus/anti-malware software on all supported systems. EnovaPoint's assets shall be protected against infection by viruses, spyware, or other malicious software.

The anti-virus/anti-malware software shall be monitored regularly to help ensure that scheduled scans are completing properly and that threat definitions are being applied daily or as they

become available from the vendor. Any issues identified should be immediately investigated and remediated.

12. Logging and Monitoring.

12.1. Logging is enabled to monitor administrative activities; logon attempts and data deletions at the application and infrastructure level. Automated alerts are configured to notify IT management and issues identified are resolved in a timely manner through the incident management process.

12.2. An enterprise monitoring system constantly monitors Production systems for capacity and usage requirements of the system. Results are reviewed and decisions made if capacity requires modification based on usage results.

13. System Development and Change management

13.1. EnovaPoint shall implement formal, documented change control procedures to manage changes to information systems, supporting infrastructure, and facilities. Major changes impacting Customer Data or supporting systems shall be communicated to Customers at least 7 days prior to implementation. Stakeholder approval shall be provided prior to change implementation.

13.2. EnovaPoint shall logically or physically separate environments for development/testing, and production. User access to environments and Customer Data, including personal data, shall be restricted and segregated, based on job responsibilities. User access to program source code shall be restricted and tracked.

13.3. Developers must be trained in secure coding techniques based on best practice guidelines. A secure coding standard must be utilized as part of the software development methodology. Appropriate requirements and controls must be in place to secure and protect application source code including, but not limited to, the following:

- Directories or repositories containing application source code are secured from unauthorized access.
- Source code is not stored on production systems when possible.
- All changes to code are logged in a central version control solution and to the extent possible, should also log all access to source code files.
- Access and modification access is properly assigned.

14. Vendor Management

EnovaPoint agreements with third parties sub-processing Customer Data shall include appropriate information security, confidentiality, and data protection requirements. Agreements

with such parties and its reassessment shall be reviewed periodically (at least every 12 month) to validate that information security and data protection requirements remain appropriate.

15. Incident Management.

Incident Management Policy. EnovaPoint shall define policy and procedures on how to respond to suspected or actual security and/or privacy incidents that result in a breach of confidential data. Incidents must be logged in Incident Register, including incident description, Severity level, Business risk type, investigation results and measures to be takes to mitigate such incident in the future. EnovaPoint shall support any investigation that involves Customer Data.

16. Resilience.

16.1. Business Continuity, Disaster Recovery. EnovaPoint shall perform business continuity risk assessment activities to determine relevant risks, threats, impacts, likelihood, and required controls and procedures. Based on risk assessment results, EnovaPoint shall document, implement, annually test and review business continuity and disaster recovery ("BC/DR") plans to validate the ability to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident that results in loss or corruption of Customer Data.

16.2. Backup and Retention Policy. EnovaPoint shall ensure that backup copies are created and retired at defined intervals and regularly tested according to documented backup and retention procedure.

17. Audit and Compliance.

17.1. Compliance. The purpose of this measure is to prevent any breach of obligations under laws, treaties and regulations. EnovaPoint shall periodically review whether its systems and equipment storing, enabling access to, or otherwise processing Customer Data, including personal data, comply with legal and regulatory requirements and contractual obligations owed to Customer. EnovaPoint management shall review the technical and organizational controls implemented to protect Customer Data for compliance with agreed-upon information security controls at least annually and report results to senior management.

17.2. Audit. Audit requirements are carefully planned and coordinated to reduce the risk of downtime. EnovaPoint shall maintain current independent verification of the effectiveness of its technical and organizational security measures (e.g., ISO certification, SOC 2 Type II). The independent information security review shall be performed at least annually.