Updated: 2023-06-23

ENOVAPOINT'S 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, aligned with the standards of ISO 27001. This policy applies to all employees and is designed to maintain the security of the organization's information. To ensure consistency, relevance, adequacy, and effectiveness, 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; (b) tailored for each area of information security (i.e., user access, system development and change, business continuity, etc.) and supplemented by specific policies as required; (c) reflects the requirements of applicable law, including Data Protection laws; (d) approved by management; (e) communicated to all employees and third-party contractors (if applicable); and (f) subject to periodic review and updates, ensuring alignment with evolving legal, operational, and risk landscapes

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. These responsibilities specifically encompass the respectful and lawful handling of all customer data, with firm obligations to avoid unauthorized disclosure, misuse, alteration, or destruction of this information, and shall survive termination or change of employment or engagement. In addition, to minimize the risk of unauthorized or unintentional modification or misuse of Customer Data, we have implemented a robust system of role-based access controls and segregation of duties. This approach ensures that individuals can only access and process the data necessary for their specific job functions, reducing the likelihood of internal threats to data security.

3. Personnel management

3.1. Background Check. As part of our comprehensive hiring process, we conduct background checks on all job applicants in compliance with applicable laws, regulations, and ethics. These checks are designed to validate the applicant's history and assess their suitability for handling sensitive information. Our aim is to ensure that all our employees have a demonstrable track record of integrity, with no known incidents related to information leakage, unauthorized disclosure of proprietary information, or similar breaches of trust.

3.2. Information Security Training. All employees must participate in regular information security training. This training program is designed to ensure they remain informed about our organization's policies, procedures, and any changes thereto that are related to their work.

4. Access Control

4.1. Access Control policy. EnovaPoint adheres to the principle of least privilege, ensuring that users only have access to the information and resources necessary to perform their job functions. This access is determined by Senior Management and reviewed quarterly to ensure alignment with current job duties. Any access found to be inappropriate or unnecessary is immediately revoked.

4.2. Password Management Policy. This policy governs the creation, use, and modification of passwords used to access EnovaPoint's and third-party vendor operating systems, applications, and data. The Company enforces a strong password policy, which includes requirements for password length, complexity, and expiration, to protect the privacy and security of data, whether at rest or in transit.

4.3. Network and Network Service Access Management. Access to Customer Data is strictly controlled and can only be made via the corporate network or through a secure VPN, with IP restrictions also applied. All employee devices are encrypted and managed remotely to ensure their security. For enhanced enterprise network security, we utilize robust mechanisms including firewalls, Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS), and Azure Sentinel.

5. Physical Security.

The EnovaPoint's office premises are secured with an alarm system, and each employee is provided with an individual office access code to ensure controlled and monitored access. The internal server room, which houses our IT infrastructure, is located separately, and is secured with its own dedicated alarm system. Entrance by non-employees is controlled and only permitted with our staff's explicit authorization. Importantly, **no Customer Data** is stored,

downloaded, or processed on the Company's physical premises or employees' computers. Instead, Customer Data is securely stored and processed within secured and isolated, customer chosen Azure data center facilities provided by Microsoft, which adhere to the highest industry standards for data security and resilience.

6. Asset Management.

6.1. Asset Register: EnovaPoint maintains an inventory of all physical and digital assets used in the organization, particularly those used to view or store confidential information. This inventory is updated annually and includes all systems connected to the network and the network devices themselves. Inventoried items range from desktop workstations, laptops, servers, network equipment (like routers, switches, firewalls), to printers, storage area networks, telephony systems, and more.

6.2. Use of Assets: All employees and third-party contractors (if applicable) are required to adhere to our documented policies on the acceptable use and handling of assets. Upon termination of employment or contract, assets must be returned immediately. The process of asset return is monitored, tracked, and verified to ensure compliance.

6.3. System Hardening: EnovaPoint has formal, documented procedures in place for system hardening and the establishment of baseline configurations. The use of unsupported software or hardware is strictly prohibited to maintain the integrity of our systems.

7. Protection of Data.

7.1. Encryption at Rest: We employ a range of encryption methods to protect any Customer Data stored at rest, adapted to suit the storage medium. These include:

- Microsoft SQL Server on Azure: Transparent Data Encryption (TDE) using the AES-256 algorithm.
- Azure Virtual Machines: We secure data with Azure Disk Encryption, also using the AES-256 algorithm.
- Azure Storage: Data is protected by Azure Storage encryption, utilizing the AES-256 algorithm.
- Microsoft 365: EnovaPoint’s internal documents, including customer quotations, invoices, and agreements, are secured both at rest (using BitLocker and DKM) and in transit (using TLS) with end-to-end encryption.
- Workstations: We use BitLocker for encrypting data on workstations.

7.2. Protection in Transit. We ensure that all confidential data, including Customer Data, transmitted across public networks, or to external entities, is securely protected and encrypted during transfer to maintain the integrity and privacy of the information. We implement robust security protocols such as HTTPS, TLS 1.2 or higher, SSL, and StartTLS for SMTP traffic to secure data in transit.

7.3. International Data Transfers. EnovaPoint keeps Customer Data within the customer-selected region (Azure data center) and refrains from transferring personal data to countries outside that chosen location.

7.4. Off-Premises and Remote Access Protection: EnovaPoint implements controls to protect equipment, information, and assets used off-premises and during remote access sessions, such as teleworking or remote administration. Policies for Teleworking, Electronic Communication, Network Protection, and IT Security Rules are implemented and strictly enforced.

7.5. Equipment Access Control: All equipment used by EnovaPoint employees in their activities is accessible only with granted rights and password protection. Users are required to use their own login keys for specialized software.

7.6. Protection of Unattended Sessions and Equipment: We require our users to secure unattended sessions and equipment. If a computer is inactive for more than 5 minutes, it needs to be manually locked. We enforce an automatic lock following 10 minutes of inactivity. For remote work, users are required to ensure that their information is protected from third-party access. Screen savers with an activated screen lock are mandated when computers are left unattended. We also enforce a clear desk and clear screen policy.

8. Cryptographic Controls.

8.1. Encryption. Customer Data, which includes personal data, is always encrypted both at rest and during transit to maintain its integrity and confidentiality.

8.2. Key Management. A secure key vault is used for key management. Encryption keys are protected to ensure access is only granted to authorized users and applications. To further enhance security, encryption keys are not stored on the same media as the data they protect. In situations where keys are stored either physically or logically near the data they secure, additional mitigating controls are implemented. Such controls may include, but are not limited to, the encryption of the keys themselves to prevent a compromise of the data.

9. Network Security

9.1. Network Segregation: EnovaPoint segregates network systems containing Customer Data from those supporting internal activities or other tasks. We ensure logical segregation of Customer Data even within a shared service environment. Network segments where Customer Data is accessible are secured from external entry points to protect against unauthorized access.

9.2. Secure Gateway: A secure gateway (Firewall) is implemented to protect and segregate the internal network from external networks or DMZs. The selected gateway conforms to industry standards and can enforce the security policies defined in our Access Control Policy.

9.3. Remote connections. All remote connections to the network hosting Customer Data are restricted to EnovaPoint's corporate IP address. For additional security, a multi-factor authentication method is enforced. The provision of users for remote access follows the guidelines set out in our Access Control and Teleworking policies.

10. Penetration Testing

EnovaPoint conducts annual penetration testing on applications that store or provide access to Customer Data, including personal data. This process is also repeated whenever significant changes are made to these applications. The latest penetration test report is made available to customers upon request.

11. Vulnerability Management

EnovaPoint implements and maintains industry-standard best practices to protect our corporate network, including but not limited to, the use of network firewalls, intrusion detection or prevention systems, and anti-virus/anti-malware software on all supported systems. This helps to protect our assets against infection by viruses, spyware, and other malicious software.

The performance of anti-virus/anti-malware software is monitored on a regular basis. This monitoring ensures that scheduled scans are completed properly and that threat definitions are updated daily or as they become available from the vendor. Any identified issues are immediately investigated and remediated.

We use Microsoft Azure for our application infrastructure hosting Customer Data, which adheres to our stringent vulnerability management protocol and operates in compliance with industry best practices for security and reliability.

12. Logging and Monitoring.

12.1. Logging Mechanism. EnovaPoint enables logging to closely monitor administrative activities, including logon attempts and data deletions, at both the application and infrastructure levels. Automated alerts are configured to promptly notify IT management of any potential issues. Identified issues are quickly addressed and resolved through a robust incident management process.

12.2. Enterprise Monitoring. We employ a dedicated enterprise monitoring system available at Azure to continuously oversee the capacity and usage requirements of our production systems. This monitoring data is regularly reviewed, and decisions to modify capacity are made based on these usage results.

13. System Development and Change management

13.1. Change Control Procedures. EnovaPoint implements formal, documented change control procedures for managing modifications to information systems, supporting infrastructure, and facilities. Significant changes that impact Customer Data or supporting systems are communicated to customers prior to implementation via in-app alerts or by email. Stakeholder approval is obtained prior to the implementation of changes.

13.2. Segregation of Environments. EnovaPoint ensures physical separation of development/testing and production environments. Customer Data in any form is not utilized in non-production environments. Access to these environments and Customer Data, including personal data, is restricted, and segregated based on job responsibilities. User access to application source code is controlled and monitored.

13.3. Secure Coding. Developers receive training in secure coding techniques following industry best practice guidelines. A secure coding standard is employed as part of our software development methodology. Several measures are in place to secure and protect application source code, including:

- Securing directories or repositories containing application source code from unauthorized access.
- Avoiding the storage of source code on production systems where possible.
- Logging all changes to code in a central version control solution. If possible, all access to source code files is also logged.
- Ensuring that access and modification permissions are appropriately assigned.

14. Vendor Management

EnovaPoint ensures that all agreements with third-party vendors involved in sub-processing Customer Data incorporate stringent information security, confidentiality, and data protection

requirements. These agreements are regularly reviewed and assessed, at least every 12 months, to verify that the information security and data protection provisions remain relevant and effective.

15. Privacy by Design and Default.

EnovaPoint is committed to embedding privacy considerations into every stage of our product development and business operations, following the principle of 'Privacy by Design'. This approach involves proactively integrating data protection measures into our system architectures, business processes, and practices from the onset, rather than as an afterthought. We adopt a 'data minimization' approach where we only collect, process, and store the minimal amount of personal data necessary for legitimate business purposes, in line with GDPR principles. In addition, our systems are designed with 'Privacy by Default' settings to ensure that, by default, personal data is not accessible to an indefinite number of individuals. Personal data is only accessible on a need-to-know basis, and default settings only allow necessary processing. Moreover, we continuously review and update our privacy-enhancing technologies to maintain their effectiveness and ensure alignment with evolving privacy norms and regulations.

16. Incident Management.

16.1. Incident Management Policy. EnovaPoint has established policies and procedures to effectively respond to suspected or actual security or privacy incidents that result in breach of confidential data. These procedures include maintaining an Incident Register, which records the incident description, severity level, business risk type, investigation results, and measures to prevent similar incidents in the future. EnovaPoint is committed to supporting any investigation that involves Customer Data.

16.2. Data Breach Notification. EnovaPoint places a high priority on maintaining the security of Customer Data, including personal data. Despite our comprehensive security measures, in the unlikely event of a data breach, we are committed to promptly informing affected parties. We have a robust Data Breach Response and Notification Procedure in place that includes defined procedures for identifying, containing, and investigating a data breach. In the event of a confirmed breach, we will notify affected customers without undue delay and, where feasible, within 48 hours after becoming aware of it. This notification will include details such as the nature of the breach, the types of information involved, the likely consequences, and the measures taken or proposed to mitigate its possible adverse effects. Our notification process complies with the requirements of applicable data protection laws, including GDPR and other regional regulations.

17. Resilience.

17.1. Business Continuity, Disaster Recovery (BC/DR). EnovaPoint is committed to conducting regular business continuity risk assessments to identify relevant risks, threats, impacts, likelihood, and necessary controls and procedures. Based on these assessment results, EnovaPoint will document, implement, and review BC/DR plans annually. These plans aim to ensure the swift restoration of availability and access to Customer Data in the event of a physical or technical incident that results in the loss or corruption of such data.

17.2. Backup and Retention Policy. EnovaPoint has a well-documented backup and retention procedure, which ensures that backup copies of data are created, stored, and retired at defined intervals. These backups are tested regularly to ensure the integrity and availability of the data.

18. Audit and Compliance.

18.1. Compliance Management. EnovaPoint is dedicated to preventing any breaches of obligations under laws, treaties, and regulations. The Company will periodically review the compliance of its systems and equipment that store, process, or enable access to Customer Data, including personal data. This is to ensure that they align with all legal, regulatory, and contractual obligations. The management of EnovaPoint will review the implemented technical and organizational controls for the protection of Customer Data at least annually. The results of these reviews will be reported to senior management.

18.2. Audit. EnovaPoint places a high priority on audit requirements, which are carefully planned and coordinated to minimize the risk of operational interruptions. The Company maintains up-to-date independent verification of the effectiveness of its security measures, including ISO certifications and SOC 2 Type II attestations. An independent information security review is conducted at least annually.