Information security exhibit

Enable maintains an all-encompassing, documented information security program that contains administrative, technical, and physical safeguards. These are designed to ensure that customer data remains secure and is handled in compliance with all regulatory requirements applicable to Enable and its SaaS Subscription Services. This Information Security Exhibit (this "***Exhibit***") applies to the SaaS Subscription Services, and all associated Enable processes, controls and systems used in the development, operation and ongoing support of those Subscription Services.

1. Corporate

A. Information Security Management System

Enable maintains an Information Security Management System (or "***Enable ISMS***") that defines Enable policies, standards, guidelines, and procedures as part of Enable's documented information security program, covering the management of information security for the Subscription Services and all related Enable internal operations. Enable ISMS is designed to:

- Establish directives and principles for action regarding information security;
- Document and maintain compliance with statutory, regulatory, and contractual requirements, including but not limited to: SOC1, SOC2, GDPR, ISO 9001 and ISO 27001; and
- Monitor, evaluate and adjust, as appropriate, considering relevant changes in technology, threats to Enable or to Customer data and security and privacy regulations applicable to Enable.

This Exhibit describes the current policies, standards, guidelines, and procedures under Enable ISMS. Enable may update or enhance the ISMS and this Exhibit at its discretion to reflect ongoing changes in law, regulation, or industry best practice there will be no material impact on the level of security described herein. .

Risk Management. Enable ISMS operates a risk management program under which Enable conducts regular risk assessments at the enterprise, customer and change level intended to anticipate threats to the security of customer data using qualitative and quantitative measures. The risks will be reviewed and updated in line with a documented schedule and expanded on as the business grows.

Change Management. Enable ISMS comprises a change management program to govern all changes to Enable production Subscription Service systems, applications, and databases, including (i) documentation, testing, and approval of all changes; (ii) security assessments of all changes prior to deployment into production; and (iii) security patching in a timely manner based on risk analysis. In addition, Enable will require all changes to Customer production environments to be documented on an approved change request prior to deployment.

Testing. At least annually, Enable reviews, audits and tests key controls, systems, and procedures of Enable ISMS to validate that they are properly implemented and effective in addressing identified threats and risks. Non-conformities are documented centrally and discussed during regular management reviews.

Asset Management. Enable ISMS retains an asset management program for all Enable assets. Each asset is identified, tagged, and registered by Enable in an asset inventory before it can be used for any business activity related to the Subscription Service. Enable classifies and labels each asset based on relevant criteria.

Business Continuity & Disaster Recovery. Enable ISMS maintains a business continuity framework designed to mitigate the risk of single points of failure and provide a resilient environment to support Subscription Service continuity and performance. Enable administers comprehensive plans for crisis management and communication, supply chain management and individualized department action strategies designed to prevent interruption of critical business functions. Enable conducts formal disaster recovery plans and cyber security incident response designed to minimize disruption to critical business operations and customer systems. Enable maintains production and disaster recovery environments to support failover procedures and redundancy requirements, as well as proactive protection and detection methods designed to limit damage from disaster events.

Incident Response. Enable ISMS operates a security incident response plan to be followed in the event of any unauthorized exposure, corruption, or loss of Customer Data (each a "***Security Incident***"). The Security Incident response plan defines personnel roles and responsibilities, as well as procedures related to Security Incident identification, containment, investigation, communication, forensic analysis, recovery and remediation, documentation, and reporting. If Enable verifies that any Customer data is impacted by a confirmed Security Incident, Enable will notify the affected Customer without undue delay to the extent permitted by law.

B. Certifications & Audits

The Enable ISMS governance controls are designed to align to the ISO 27001 framework as well as the Trust Services Criteria of SOC 1 and 2. Enable maintain an internal audit program and require annual independent third-party assessments for continued certification purposes. An independent third party will audit the Subscription Services annually for compliance with the following standards (or their successor equivalents):

- SOC 1 Type II
- SOC 2 Type II
- ISO 9001; and
- ISO 27001.

Enable will provide the active customer, upon request, with a copy of the relevant ISO certificate or SOC Report.

Enable conducts internal audits designed to monitor Enable ISMS compliance on an ongoing basis. Enable will review and modify internal audit controls based on a risk-based approach that impact assesses changes in legislation, regulations, certification standards, internal audit findings, observations and industry best practices.

C. Personnel

Confidentiality & Ethics. Enable will require all Enable employees to

(i) sign a confidentiality agreement as a condition of employment, and

(ii) annually confirm compliance with all relevant laws, regulations, corporate policies, and industry best practices for ethical corporate interactions by signing the Enable Code of Business Conduct and Ethics within the employment terms and conditions. Enable ISMS requires contractors with access to Enable systems or Customer data to be subject to the same confidentiality and ethical obligations as those required of Enable employees.

Training. Enable ISMS conducts mandatory security awareness and training programs for all Enable personnel at induction with tailored training sessions on a quarterly basis, specifically designed to promote a culture of security awareness. Enable provides additional role-based security training to Enable personnel as appropriate. Enable trains employees who have access to sensitive data in relevant laws and regulations. Enable ISMS requires contractors with access to Enable systems or customer data to complete the same security awareness training and commitment to Enable information security policies as those required for Enable employees.

2. System Controls

A. Access. Enable ISMS includes policies, procedures and logical controls designed to restrict access to Enable networks, systems and all elements of the Subscription Service (including customer data) on a need-to-know basis and based on the principle of "least privilege."

Enable (i) electronically monitors and manages active access privileges.

(ii) verifies business justification for access requests;

(iii) limits duration of access; and

(iv) promptly removes access in the event of a change in job responsibilities, job status or otherwise when access is no longer needed working on the principle of least privilege, granted only essential access. Enable secures access points via the use of unique identifiers; password complexity in line with the United States National Institute for Standards and Technology's (NIST) guidelines regularly scheduled password updates and, where deemed appropriate, multi-factor authentication (MFA).

B. Intrusion Detection and Prevention. Enable ISMS incorporates policies, procedures and logical controls designed to limit unauthorized access to and within the Enable internal network application layer firewalls and local network intrusion prevention. Enable maintains intrusion-detection or intrusion-prevention systems (IDS/IPS) to monitor network traffic and system operations including:

- Enable environments that host systems processing, transmitting, or storing customer data;
- Internet-facing network segments; and
- Network entry and exit points for third party connections.

Enable configures and maintains all IDS/IPS devices in accordance with Enable ISMS standards consistent with industry best practices and security vendor recommendations.

C. Malware. Enable ISMS includes layered protection designed to prevent malware across Enable systems, including those supporting customer environments. Enable uses a combination of client-based threat prevention and trust enforcement (such as trusted change modelling and predictive threat prevention) and network-based threat identification and threat interruption (such as network-embedded anti-virus protection and dynamic threat detonation).

D. Monitoring. Enable ISMS will include a comprehensive program of network-wide monitoring, including the Subscription Service. Enable promptly investigates and responds to any reported anomalies. Network monitoring extends to performance monitoring and tuning, capacity planning and resource allocation designed to continuously adjust to meet changing legislative, regulatory, contractual, and business requirements.

E. Logging. Enable ISMS includes a logging platform designed to enable security review and analysis under which all Enable systems (including firewalls, routers, network switches, operating systems, and applications) log information to a centralized log server. Enable configures monitors of critical systems to alert system administrators to events that could indicate a Security Incident or a failure of security systems to operate as designed. Enable regularly reviews log files for trend analysis and pattern identification.

F. System Hardening. Enable ISMS incorporates a program for hardening operating systems designed to promptly disable unnecessary ports, protocols, and services and to apply security measures to meet baseline security configuration requirements for all infrastructure

components, including network and server elements. Enable evaluates new Subscription Service implementations for compliance with Enable ISMS baseline security configuration requirements, documenting any deviation(s) from such baseline security configuration requirements and secure appropriate approval before the affected system is deployed into production.

G. Penetration Testing. Enable engage an independent third party to conduct penetration testing ("ethical hacking") of Enable systems every 18 months as a minimum. The process of penetration testing is, on its surface, almost identical to actual hacking. The tools and techniques typically employed by malicious hackers are used by testers in order to discover system vulnerabilities and highlight potential risks. In Enable's case, the potential vulnerabilities of a web-based SaaS platform are the primary point of focus. Enable provides the applicable pen-testing Letter of Attestation to customers upon request.

H. Vulnerability Assessment & Remediation. Enable retains an independent third party to conduct both internal and external vulnerability scans on a periodic basis. Enable tracks all identified vulnerabilities, and then prioritize and address identified vulnerabilities using a risk-based model.

3. Physical Controls

A. Access. Enable ISMS includes policies, procedures and logical controls designed to limit access to Enable facilities to properly authorized individuals, including through:

(i) 24/7 CCTV monitoring of access to secure server room area of the data centre; keys are securely maintained in IT Office with controlled access by designated personnel only.

(ii) camera surveillance systems at all entrance points; and

(iii) single data centre ingress and egress point from data storage and processing facilities.

B. Environmental Security. Enable ISMS maintains environmental controls to detect and help prevent compromise or destruction of data centres, including

(i) fire, heat, and smoke detection; and

(ii) Uninterruptible Power Supply (UPS) modules;

4. Data Controls

A. Access. Enable ISMS incorporates policies, procedures and logical controls designed to:

(i) limit access to Customer Data to authorized persons,

(ii) help protect against Customer data being moved, modified or compromised, and

(iii) handle Customer data with the highest level of security and confidentiality.

B. Encryption. Enable ISMS includes policies, procedures and logical controls designed to enforce encryption on all externally accessible systems and communications:

(i) administers encryption protocols designed to isolate network communication between an application host and a database host;

(ii) provide access to the internet-facing Enable web port (for HTTPS) through network firewalls,

(iii) secure volume-based encryption of data-at-rest using keys stored separately from the data; and

(iv) secure all endpoints using encryption, password protection and remote deactivation capability.

C. Segregation. The Subscription Services operate in a multi-tenant architecture designed to segregate and restrict Customer Data access based on business needs. Enable ISMS contains policies, procedures and logical controls designed to:

(i) logically separate each Customer's data (i.e. separate database schemas) on the Subscription Service from all other Customers' data;

(ii) prevent the replication of production data for use in non-production environments without the express permission of the data owner; and

(iii) identify, secure, and manage test environments that contain production data with the same level of security as production environments.

D. Transmission. Enable ISMS maintains policies, procedures and logical controls designed to prohibit unencrypted connections into or out of the Subscription Service. Enable will encrypt Subscription Service data transmissions via an AES (or its direct successor standard) by default and protect Data in Motion using TLS1.2 (HTTPS or SFTP) (or its direct successor standard).

E. Geolocation. Enable utilizes data centres in the UK, US, Europe. Enable complies with applicable laws governing cross-border transfers and put in place cross-border transfer agreements to the extent necessary.

F. Backups. Enable ISMS incorporates policies, procedures and logical controls designed to

(i) back up Customer systems and data daily to geographically separated, encrypted servers; and

(ii) prohibit storage or archival of data on backup tapes or mobile devices.

G. Minimization. Enable ISMS includes policies, procedures and logical controls designed to ensure Customer data is processed only as instructed by the Customer.

H. Destruction. Enable ISMS includes standards for secure destruction of data consistent with current industry standards and guidance. Enable will purge Customer data in compliance with applicable law and the applicable Customer contract.

5. Other Best Practices

A. Coding Standards. Enable ISMS maintains policies, procedures and logical controls designed to ensure developers meet industry best standards of quality and use industry best security practices for Systems/Software Development Lifecycle, including a focus on the OWASP top 10 vulnerabilities.

B. Supply Chain Management. Enable ISMS contains policies, procedures and logical controls designed to ensure each third-party supplier that:

(i) acts as a data sub-processor,

(ii) stores or processes data that is critical to Enable operations, or

(iii) provides contracted staffing for roles with access to Enable systems or Customer data, complies with security standards similar to or more stringent than those set by Enable ISMS.

Last Updated: May 20, 2022