Information Security Agreement

Table of Contents

1. Introduction. This Information Security Agreement (the "ISA") is incorporated by reference to that certain agreement between the Customer and symplr software, LLC, a Texas limited liability company, or its Affiliate ("symplr"), (each a "Party"), which governs Customer's use of the applicable symplr Solution(s) (the "Agreement"), and symplr's obligations to safeguard and maintain the security of data it stores, receives, maintains or has access to on behalf of Customer. Capitalized terms used in this ISA and not defined in the Agreement are defined herein or in Section 2 below.

2. Definitions.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a Party, where "control" means the ownership of more than 50% of an entity's voting securities.

"Customer" means the entity listed on the Order which is purchasing symplr Solutions and/or Services from symplr.

"Confidential Information" has the meaning set forth in the Agreement and includes Customer Data and Personal Information. For the avoidance of doubt, any audit information, policies, and procedures provided by symplr to Customer under this ISA or the Agreement will be deemed symplr's Confidential Information.

"Customer Data" has the meaning set forth in the Agreement and for the avoidance of doubt includes data of customer that is protected health information ("PHI"), personally identifiable information ("PII") including individually identifiable health or financial information, payment card information.

"Personal Information" means Customer Data that meets any of the following criteria: (i) it identifies or can be used to identify an individual (including names, signatures, addresses, telephone numbers, email addresses, government-issued identification numbers, and other unique identifiers ; (ii) financial account numbers, credit or debit card numbers, or credit report information, access code, personal identification number, or password that would permit access to an individual's account; (iii) biometric, genetic, health, medical, or medical insurance information; or (iv) it can be used to authenticate an individual (including employee identification numbers, government-issued identification numbers, passwords or PINs, user identification and account access credentials or passwords, answers to security questions, and other personal identifiers). Customer's business contact information is not by itself deemed to be Personal Information.

"Security Incident" means any successful, actual, unauthorized access, use, manipulation, and/or destruction, including disclosure or theft of information or interference with system operations in an information system that involves Customer Data. As used herein, Security Incident does not include activities such as pings and other broadcast attacks on symplr's firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, so long as no such incident results in unauthorized access, use, or disclosure of Customer Data.

"symplr Solution" means any/all products and/or services provided by symplr to Customer, including, but not limited to SaaS, Maintenance, and Services.

3. Information Security Program.

3.1 General. symplr shall implement, maintain, and adhere to a comprehensive security program under which symplr documents, implements and maintains the physical, administrative, and technical safeguards designed to protect the confidentiality, integrity, availability, and security of Customer Confidential Data. Said security program will comply with applicable industry standards, laws, regulations, and the requirements of the ISA. Notwithstanding the foregoing, the parties acknowledge that best practices, laws, rules and regulations regarding data security and data privacy may change over time and consequently, symplr may modify its practices described in the ISA so long as such practices shall not be any less protective than the practices described herein.

3.2 Education/Awareness. symplr shall use reasonable efforts to ensure that all employees, subcontractors, agents and other parties acting on behalf of symplr ("Authorized Personnel") are aware of and comply with symplr's security policies. All Authorized Personnel must participate in security awareness training at least annually and new Authorized Personnel must undergo training prior to accessing Customer Data.

3.3 Incident Response. symplr shall have an Incident Response Plan ("IRP") in place. The IRP must detail the procedures to be followed in the event of a Security Incident. The IRP will include escalation procedures and a process for notifying the Customer within seventy-two (72) hours. symplr shall provide a detailed written report regarding the Security Incident addressing how, where, when, and what. symplr agrees to keep Customer informed of all progress and actions taken in connection with symplr's investigation of any Security Incident. Unless such disclosure is mandated by applicable law or regulation, Customer, in its sole discretion, shall determine whether to provide notification to customers, employees, or agents concerning a breach or potential breach involving Personal Information.

3.4 Network Monitoring and Reporting. For all applications and systems associated with the access of Customer Data, symplr shall generate audit logs detailing use and access. symplr shall notify Customer if a review of the audit logs reveals reasonable evidence of a Security Incident. symplr shall investigate suspected Security Incidents involving Customer Data. In the event of a Security Incident, symplr shall, within 72 hours, notify Customer and provide detailed written information regarding the Security Incident.

3.5 Company Risk Assessment. As part of its information security program, symplr or a nationally recognized auditing firm on symplr's behalf (who is subject to confidentiality obligations) has performed security assessments based on industry standards no more than one year prior to the agreement effective date and will be performed at least annually. symplr shall use reasonable efforts to address audit findings in accordance with regulatory requirements and industry standards.

3.7 Audits. Upon written request and no more than once annually, symplr agrees to provide a copy of its SOC2 or other assessment report(s) or supporting documentations (e.g., pre-populated questionnaires) similar in scope (any confidential information of symplr, not relating to Customer can be redacted) to Customer as they become available during the Agreement, at no cost to Customer. Should Customer require a custom questionnaire or security assessment, symplr may provide such questionnaire or assessments at symplr's then-current Professional Services hourly rate, provided that Customer may not request such questionnaires or assessment more than once every twelve (12) months.

3.8 Asset Management. symplr shall maintain industry standard asset inventory, device management, information classification, handling, and destruction policies and procedures.

3.9 Change Management. symplr shall maintain and follow industry standard change management procedures. symplr shall use commercially reasonable efforts to ensure that any changes to systems do not negatively impact the security of Customer Data.

3.10 Requesting and Transferring of Customer Data. symplr shall request only such Customer Data as is necessary to exercise its rights and to perform its obligations under the Agreement. The processes for data transmission between Customer and symplr will be designed and implemented to use the least Customer Data necessary. All handling and physical transfer of Customer Data shall be carried out using best industry methods appropriate to the sensitivity and criticality of the information. The process for the handling and physical transport of Customer Data must be documented. Upon Customer's written request and within thirty (30) days of physical transport, such documentation will be made available to Customer for review onsite at the applicable symplr location. Appropriate physical controls include professionally trained security personnel, Closed Circuit Television (CCTV) of transportation and processing facilities, secured lock boxes and extensive tracking, and auditing of all packages containing Customer Data.

3.11 Retention of Customer Data. symplr shall support Customer in meeting the applicable regulatory data retention requirements.

4. Information Security Infrastructure.

4.1 Access Controls. symplr shall ensure appropriate access controls are in place to protect Customer Data, including the requirements below:

4.1.1 Passphrase and Password Requirements. symplr and Customer passphrases and passwords that grant access to Customer Data shall comply with these access control standards. Passphrase and password complexity must contain the following elements:

- Passphrase and password length minimums;
- Passphrase and password complexity;
- The ability to restrict use of previously used passphrase and password;
- Passphrase and password must have an expiry;
- Account lockout must occur after a maximum number of failed password entry attempts;
- Minimum account lockout duration after a period of inactivity;
- Passphrase and password must not be transmitted or stored in plain text;
- Each user must use a unique username and passphrase and password;
- If employees, administrators, or third parties access the network remotely, remote access software must be configured with a unique username, passphrase and password, multifactor authentication, and encryption; and
- Application and operation systems default accounts and passphrase and password must be disabled or changed on production systems that support the services provided to Customer prior to symplr putting such system(s) into production.

4.1.2 Access Justification/Authorization Process. symplr authorization procedures shall comply with the following standards:

- symplr shall implement a process that ensures only Authorized Personnel are granted access to Customer Data, and that such authorization is limited to those having a business need for symplr to fulfill its obligations to Customer under the Agreement.
- Each authorization shall be reviewed by the appropriate management personnel.
- symplr shall implement a process that will immediately remove all access to Customer Data for employees that leave the company, or change positions within the company, and no longer require access. If any individual among the Authorized Personnel no longer requires access to Customer Data, symplr shall take immediate steps to remove the access of that individual.
- Annual re-verification of individuals that have access to systems that host Customer Data shall be performed to ensure that malicious, out-of-date, or unknown accounts do not exist.
- symplr shall ensure that accounts used by third-party vendors for remote maintenance are enabled only during the time needed by that vendor.
- symplr shall ensure that group, shared, or generic accounts and passwords are prohibited.

4.2 Encryption. Encryption shall be required if Customer Data is transmitted over public networks, or the use of encryption is mandated by law or regulation. Where Customer Data is transmitted over public networks or over private or public wireless networks, symplr shall use strong cryptography and encryption techniques to safeguard sensitive Customer Data. symplr shall not permit wireless access points in the production environment that hosts Customer Data.

4.3 System Security. symplr shall have commercially reasonable network intrusion detection, firewalls and anti-virus/anti-malware protection in place. symplr shall ensure that all systems that are associated with Customer Data are patched within a commercially reasonable time period after symplr has actual or constructive knowledge of any security vulnerabilities. symplr will take commercially reasonable steps to ensure that any software, systems, or networks that may interact with Customer's systems or Customer Data do not become infected by any computer viruses or other harmful components. System hardening and configuration requirements shall meet industry standard practices.

4.4 Intrusion Detection. symplr shall implement intrusion prevention systems to monitor all network traffic associated with access, processing, storage, communication, and transmission of Customer Data. Authorized Personnel will be alerted to suspected compromises and must keep all intrusion prevention systems up to date.

4.5 Security Logs and Audit Trails. symplr shall ensure that all systems storing, or processing Customer Data have logging enabled to a respective log system or a centralized log server. symplr shall actively monitor logs to identify suspected unauthorized or malicious activity to facilitate incident response. symplr shall maintain logs in alignment with the symplr Record Retention Schedule.

4.6 Network Security symplr's computer network connections, including wireless connections, are equipped with intrusion prevention capabilities, and include firewall protection and intrusion detection in accordance with applicable industry best practices. symplr maintains monitoring capabilities to ensure that: (i) system weaknesses are detected, (ii) anomalous user activity is recognized, and (iii) Vendor is informed of newly discovered vulnerabilities. symplr performs annual vulnerability scanning and third-party penetration testing.

4.7 Patch and Vulnerability Management. symplr shall ensure that all system components and software have the latest vendor-supplied security patches, using a risk-based approach, within commercially reasonable timeframes as required by its internal vulnerability management policy. symplr shall maintain intelligence feeds or processes to identify newly discovered security vulnerabilities (e.g., subscribe to alert services freely available on the Internet) and shall update standards to address new vulnerability issues.

4.8 Antivirus and Malware. symplr shall install and maintain antivirus software to protect Customer Data from viruses, worms and other damaging programs. Virus-screening software shall be maintained on all systems that access Customer Data. Antivirus software must be regularly updated with virus signatures in order to protect against new viruses.

4.9 System Hardening. symplr shall implement industry best practices with respect to system hardening on systems hosting Customer Data including:

4.10 Physical Security. symplr shall ensure that physical security measures are in place to control physical access to any systems and records that contain Customer Data. For so long as the symplr is in possession of Customer Data, symplr shall physically store all records and media containing Customer Data in an area where access can be limited to Authorized Personnel only.

4.11 Recovery Requirements.

4.11.1 Data Recovery. symplr shall have the ability to recover Customer Data in the event of a disaster. symplr shall have a written policy ("Data Recovery Policy"), covering back up copy procedures for Customer Data. For the term of the Agreement, and always while in possession of Customer Data, the Company shall maintain the Data Recovery Policy, and shall safeguard the back-up copies in accordance with such Data Recovery Policy, using the same format and a method at least as secure as the Data Recovery Policy format and methods.

4.11.2 Business Continuity Management. symplr shall maintain a written business continuity plan, to support continued business operations in the event of a business disruption or disaster declaration. The business continuity plan will be reviewed periodically, but no less than once every twelve (12) months.

4.11.3 Backup Data Storage. symplr shall adhere to the security measures stated in this ISA to securely backup Customer Data.

4.12 Information Disposal and Hardware Sanitization. Upon Customer's written request, symplr shall sanitize hard drives that contain Customer Data using industry best practices. Paper records containing Customer Data shall be disposed of in a secure manner, including one or more of the following methods: shredding, incinerating, redacting, or otherwise modifying the Customer Data contained in those documents and records to render it unreadable, undecipherable, or unrecoverable, as defined by industry best practices.

4.13 Software Development. symplr shall employ reasonable processes consistent with industry best practices for change management, secure coding principles, code inspection and review (including peer review), software development lifecycle, secure code repositories, repeatable builds, separation of development and production environments, testing plans, and code escrow. Code inspections must include a comprehensive process to identify vulnerabilities and malicious code. In addition, symplr shall ensure that processes are

documented and implemented for vulnerability management, patching, and verification of system security controls prior to their connection to production networks.

5. Precedence. If any provision of the ISA and any provision of the Agreement are inconsistent or conflicting, the ISA shall control, but only to the extent of such inconsistency or conflict.