Entrust Corporation
Vendor Information Security Addendum

Introduction

Vendor and Entrust Corporation ("Entrust") have entered into an agreement under which Vendor has agreed to provide services and/or products under the terms of that agreement ("Agreement"). Vendor agrees that it shall comply and cause any third-parties acting on its behalf ("Third Parties") to comply with the information security terms contained herein ("Vendor Information Security Addendum"). This Vendor Information Security Addendum is incorporated in and made a part of the Agreement.

Definitions

Unless otherwise set forth in the Agreement, the following definitions shall apply to this Vendor Information Security Addendum:

"Confidential Information" shall have the meaning set forth in the Agreement between the Entrust and Vendor provided however, that in any event, Confidential Information includes Personal Data, as defined below.

"Data Protection Laws" means all applicable data protection and data privacy laws and regulations, including but not limited to the EU General Data Protection Regulation (GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the California Consumer Privacy Act (CCPA).

"Entrust Policies" means all Entrust policies, standards, guidelines and rules in force from time to time which Entrust has communicated to Vendor or its employees.

"Data Security Breach" means an actual or suspected unauthorized: disclosure , access, acquisition, processing, transfer, or disposal of, Confidential Information or Entrust's systems.

"Personal data" shall have the meaning ascribed to "personally identifiable information," "personal information," "personal data" or equivalent terms as such terms are defined under Data Protection Laws.

"Processing" or "Process" means any operation or set of operations that is performed on Confidential Information, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmissions, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Security Policy" has the meaning given to it in paragraph 2.1.

Vendor agrees to establish and maintain and shall require its Third Parties to establish and maintain the following safeguards to ensure the security of Entrust's Confidential Information:

1. General Terms

1.1. For the term of the Agreement and for so long as Vendor holds Entrust's Confidential Information or may impact the security of Entrust's systems, it will take all take all reasonable steps to ensure the confidentiality, integrity, and availability of Entrust's Confidential Information and systems. Vendor shall not disclose any Confidential Information to any unauthorized third party without the express written permission of Entrust.

1.2. Vendor shall comply with all applicable privacy and Data Protection Laws.

1.3. To the extent Vendor processes cardholder data, as defined by the PCI Security Standards Council, Vendor acknowledges it's required at all times to secure such cardholder data and agrees to comply with applicable Payment Card Industry Data Security Standard requirements (PCI DSS) and shall provide a copy of its current PCI-DSS attestation of compliance, upon request.

2. Information Security Program

2.1. Vendor shall develop, implement and maintain a comprehensive, written information security program that is reviewed and updated at least annually (the "Security Policy") in accordance with: (i) industry recognized standards and best practices, such as ISO 27001, NIST 800-53, PCI-DSS, etc.; and (ii) Data Protection Laws. Upon request, Vendor shall make available to Entrust a copy of its Security Policy. Vendor shall designate an employee or employees to coordinate and implement the Security Policy. The Security Policy shall have been approved by senior management of Vendor. Vendor's employees and agents who have access to Vendor's systems shall be required to review and accept the Security Policy, at least annually.

2.2. The Vendor shall perform, or cause a reputable third-party to perform, comprehensive penetration tests and code review with respect to Vendor's information systems at least annually or whenever there is a material change in technical or organizational measures. The penetration tests, code reviews, and such other information security assessments and threat and vulnerability assessments shall cover the following:

2.2.1. the identification and evaluation of risks that could result in unauthorized Processing of Confidential Information or inability to Process Confidential Information;
2.2.2. the assessment of the adequacy and effectiveness of security measures; and
2.2.3. a gap analysis in order to prevent leakage, alteration or damage of Confidential Information.

2.3. For each test and assessment, Vendor shall review the results and update its security measures and training in order to remediate any risks identified in the test or assessment. Such remedial efforts shall be taken with urgency in accordance with industry recognized standards and the sensitivity of the risk. Upon request, Vendor shall provide reasonable updates on remedial efforts to Entrust.

2.4. Upon request, Vendor shall provide to Entrust an executive summary report containing the results of the penetration tests and vulnerability assessments described above along with remedial steps taken.

2.5. Vendor shall procure the performance of information security risk assessments by independent third parties or internal personnel independent of those who develop or maintain Vendor's information systems or information security program.

2.6. Vendor shall continuously review and assess its Security Program to ensure adequacy and alignment with industry recognized standards.

3. Human Resource Management

3.1. Vendor shall, to the extent permitted by law, conduct prior to hire comprehensive background checks, including: criminal record, employment history, reference checks, and other industry appropriate requirements to ensure reliability and personal integrity of all employees, agents, and contractors.

3.2. Vendor shall not allow any employee or third party who has failed to pass a background check to have access to Confidential Information or be involved with performing services for Entrust.

3.3. At the time of hire and annually thereafter, Vendor shall ensure that all employees and third parties with access to Confidential Information or are involved with providing services to Entrust have completed appropriate training on Vendor's information security program and obligations to ensure the security of Confidential Information. Vendor shall continuously provide appropriate supervision and guidance to ensure that security is at the forefront of the minds of its employees.

4. Data Security Breach Notification

4.1. Vendor shall notify Entrust, without undue delay, and in no event later than forty-eight (48) hours, of Vendor becoming aware of any Data Security Breach to soc@entrust.com. In Vendor's notice, Vendor shall specify to the extent available:

4.1.1. the time, date and location of the incident and a description of the nature of the incident, including a description of affected and potentially affected Confidential Information;
4.1.2. an assessment of the likely consequences of the incident;

4.1.3. measures taken and/or to be taken to mitigate the consequences of the incident; and

4.1.4. any other information reasonably required by the Entrust relating to the incident from time to time.

5. Security Incident Management

5.1. Vendor shall maintain an incident management process for addressing information security incidents and Data Security Breaches, including escalation paths to senior management, incident contact lists, initial responses, investigation log, system recovery, issue and eradication, reporting and review and follow up procedures, including appropriate notification to regulators and law enforcement.

5.2. Vendor's incident management process shall include a recording of relevant detail, which may include: the type of incident, date and time of the incident, the person who reported the incident, the cause and effect of the incident, and the remedial actions taken in response to the incident.

5.3. Vendor shall utilize a lessons learned exercise to improve its security program, which shall include documenting the areas identified for improvement, and the actions taken. Upon request, Vendor shall provide a copy of its lessons learned exercise documentation.

6. Physical and Environmental Security

6.1. Vendor shall maintain Vendor's information systems in a physically secure environment safe from physical and natural threats, which shall include:

6.1.1. physical entry controls, which are reasonably appropriate in the circumstances, to ensure that only authorized individuals gain access to such facilities; and

6.1.2. environmental controls, which are reasonably appropriate in the circumstances, to protect against damage from fire, water, or other environmental hazards

6.2. Vendor shall limit access by using physical barriers which shall be controlled either through electronic access control validation (e.g. keycard) or validation by human security personnel (e.g. security guard.). Employees and other third parties shall wear photo-ID badges at all times while at the facilities.

6.3. Vendor shall ensure that visitors shall be required to sign-in, show appropriate identification, and assigned a visitor ID badge that must be worn while the visitor is at any of the facilities, and shall be continually escorted while visiting the facilities.

6.4. Vendor shall only provide access to its facilities on a need to know and least privilege basis. Access privileges shall be promptly revoked when the need no longer exists.

6.5. Vendor shall ensure that all access points to the data processing facilities shall be maintained in a secured state and monitored by video surveillance cameras that will record all individuals accessing the facilities. To the extent permitted by law, Vendor will retain video surveillance footage for one hundred and eighty (180) days. Vendor shall also maintain electronic intrusion detection systems that will detect unauthorized access to the facilities. All physical access to the facilities by employees and third parties shall be logged and routinely audited.

6.6. Vendor shall maintain throughout data processing facilities fire, smoke, heat, and water detection and non-water based fire suppression mechanisms (e.g. Class C). Vendor shall ensure that fire hazards, such as cardboard are not permitted in the data processing facilities. Where appropriate, Vendor shall maintain power backup systems to ensure uninterrupted power supply.

7. Business Continuity and Disaster Recovery

7.1. Vendor shall develop and maintain business continuity and disaster recovery plans to ensure the continuity of services provided to Entrust. The business continuity and disaster recovery plans shall be reviewed and tested annually. Upon request, Vendor shall provide evidence of its completed business continuity and disaster recovery tests.

7.2. Except as otherwise required by industry standards, law, or the Agreement, Vendor shall backup all Confidential Information daily. Vendor shall maintain a recovery point objective of no less than twenty-four hours (24) hours and recovery time objective of no less than seventy-two (72) hours. Backup data shall be encrypted as set forth by the requirements in this Vendor Information Security Addendum.

8. Transportation and Encryption

8.1. Vendor shall implement and maintain appropriate controls to avoid the theft, loss or unauthorized access of Confidential Information during the transportation or transfer of media or documents by making prior arrangements with the intended recipient to secure the receipt of Confidential Information.

8.2. Vendor shall encrypt all Confidential Information, using at least 256-bit symmetric or 2048-bit asymmetric encryption both in transit and at rest. Vendor shall manage encryption programs and encryption keys to prevent leakage and unauthorized and improper use.

9. Access Management

9.1. Vendor shall make Confidential Information available only to its employees or third parties who have a legitimate business need to access Confidential Information in order to assist Vendor carry out its obligations under the Agreement.

9.2. Vendor shall have a formal user access management process for those with access to Vendor's facilities and systems, including identification and authentication controls that:

9.2.1. requires formal periodic review and approval;
9.2.2. grants access only on the need to know and least privilege basis;
9.2.3. utilizes multi-factor authentication for remote network access;
9.2.4. access is revoked or disabled after ninety (90) calendar days of inactivity;
9.2.5. revokes access immediately after termination or no longer needed;

9.3. Vendor shall ensure that only employees with the appropriate permissions set out in Vendor's Security Policy have the ability to grant, alter or authorize the access rights to Vendor's information systems.

9.4. Vendor shall use industry recognized authentication protocols, including assigning unique identifications, multifactor authentication, and strong passwords. Password and authentication controls shall include:

9.4.1. Any default password shall be changed immediately.
9.4.2. Passwords shall be encrypted in transit and storage.
9.4.3. Passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties are not able to observe or subsequently recover them. Passwords must not be logged or captured as they are being entered. Passwords shall be stored, salted and hashed, and not in clear text.
9.4.4. Password must at a minimum be no less than ten (10) characters. Password complexity level should not be less than 3 out of 4 character types and must have character type choices such as upper case letters, lower case letters, numeric digits, or special characters (such as $, !, #, %, etc.).
9.4.5. The last five (5) passwords cannot be reused. Passwords must be changed every ninety (90) days.
9.4.6. Passwords must not be shared.
9.4.7. Passwords associated with privileged accounts must be stored in a password vault.

9.5. Vendor shall block user access after no more than five (5) unsuccessful attempts to gain access and timeout after thirty (30) minutes of inactivity for all systems and applications that store Confidential Information.

9.6. For all systems that Process Confidential Information, Vendor shall maintain a complete record of access requests and log activity on those systems. Such records and logs shall be maintained for at least one (1) year or as otherwise required by law. Vendor shall maintain a process to systematically review such records.

9.7. Vendor shall routinely inspect the logs of relevant access events and shall store all logs in separate physical devices and back up such data regularly.

9.8. Vendor shall implement strong authentication mechanisms, such as multi-factor authentication, for all remote access to Vendor's network, systems and applications that store Confidential Information. Additionally, remote access activity shall be logged and monitored.

9.9. Vendor shall ensure that responsibility for information security management under the Agreement is clearly assigned by an individual with appropriate skills, experience, and influence in the organization. Vendor shall ensure separation of duties as appropriate and applicable.

9.10. Vendor shall maintain measures using either physical or logical access controls to separate Entrust Confidential Information from Vendor's or Vendor's other clients' information.

9.11. Vendor shall maintain clean desk/clear screen policies and ensure unsecured Confidential Information is not left unattended to protect against the unauthorized, viewing, copying, alteration, destruction or removal of media containing Confidential Information.

9.12. Vendor shall regularly perform social engineering tests (i.e. simulated phishing exercises), to determine compliance with Security Policy and take remedial actions where appropriate.

9.13. Vendor shall implement and maintain appropriate data leak prevention controls (e.g. by prohibiting devices and disabling functionality or protocols that allow uncontrolled exfiltration of Confidential Information).

10. Network Security Controls

10.1. Vendor shall protect Confidential Information in its networks against unauthorized access or modification, by using, network security devices, such as firewalls and intrusion detection and prevention systems, at critical junctures of Vendor's IT infrastructure to protect the network perimeters.

10.2. Vendor shall use up-to-date versions of system security software including firewalls, proxies, web application firewalls and interfaces. Additionally, Vendor shall implement and maintain up-to-date antivirus software, malware protection, security updates, patches, and virus definitions consistent with industry recognized standards. Such software shall be installed and running to scan for and promptly remove viruses on all endpoints, servers and networks.

10.3. Vendor shall maintain a patch management process that requires that patches are tested before installation on all systems that Process Confidential Information or are used to deliver services to Entrust.

10.4. Vendor shall ensure that system administrators maintain complete, accurate, and up-to-date information regarding the configuration of all systems that handle Confidential Information.

10.5. Vendor shall maintain controls to ensure the timely identification of vulnerabilities in Vendor's information systems, including intrusion detection and/or prevention and monitoring and response processes, which identify both internal and external vulnerabilities and risks. At least monthly, Vendor shall scan its information systems with industry-standard security vulnerability scanning software to detect security vulnerabilities. Vendor shall classify detected vulnerabilities according to CVSS and shall remediate any such vulnerabilities within commercially reasonable timeframes commensurate with the risk or severity rating.

10.6. Vendor shall subscribe to vulnerability intelligence services that provide current information about technology and security vulnerabilities.

10.7. Vendor shall refrain from storing Confidential Information on media connected to external networks unless necessary for business purposes.

10.8. Vendor shall log network and remote access attempts and maintain those logs for a minimum of six (6) months.

10.9 To the extent Vendor requires access to Entrust's network, systems, or computing environment, Vendor must follow Entrust's security policies and controls and utilize Entrust provided hardware and access mechanisms to connect to Entrust's network, systems, or computing environment. Vendor shall not connect third party devices to Entrusts network, systems, or computing environment, unless mutually agreed upon in a statement of work and approved by Entrust's CISO.

11. Third Party Management

11.1. Vendor shall ensure that any authorized Third-Party is at all times contractually bound by substantially similar obligations as set forth in this Vendor Information Security Addendum and shall conduct regular due diligence of said Third-Party to ensure continued compliance with the terms. Vendor shall immediately notify Entrust if it suspects or confirms that Vendor's Third-Parties are out of compliance with the requirements set forth herein.

12. Temporary File Management

12.1. Vendor shall ensure that temporary files containing personal data:

12.1.1. Adhere to data minimization principles
12.1.2. Are created only where strictly necessary
12.1.3. Are protected to a level consistent with the original information
12.1.4. Are retained only for as long as required for processing; and

12.1.5. Are erased once processing ends.

12.2. Vendor shall make every effort to avoid temporary files being written to backup storage. In cases where such backups are unavoidable, in whatever media format and howsoever made, Vendor shall scan for such temporary files at least annually and prior to the end Vendor's engagement with Entrust, and security delete the data so that it cannot be retrieved.

13. Asset Management

13.1. Vendor shall implement a documented process and tools for tracking both physical and data assets, which should include:

13.1.1. a process for recording the receipt of documents or media containing Confidential Information to include appropriate identifiers associated with the document or media; and

13.1.2. a process for recording any outgoing documents or media containing Confidential Information to include appropriate identifiers associated with the document or media.

13.2. Vendor shall maintain a data classification policy to indicate the level of sensitivity assigned to data and ensure appropriate level of protection is applied accordingly. Whenever practicable, Vendor shall label confidential information as such. Vendor acknowledges that Confidential Information is and shall remain confidential and owned by Entrust irrespective of labeling or absence thereof.

14. Software Lifecycle Management

14.1. Vendor shall abide by industry-standard application development and coding practices and processes (e.g. OWASP Top 10) to ensure the security and integrity of applications and prevent source code from unauthorized and untested alterations.

14.2. Vendor shall not use any Confidential Information in development and test environments unless protected to the same level as in the production environment and the requirements set forth in the Agreement.

14.3. Vendor represents and warrants that any software provided under the Agreement is free of any known viruses, malicious or backdoor code, undisclosed features designed to access, disable, damage, impair, erase, deactivate or electronically repossess Confidential Information or Entrust's environment, and is appropriate for its intended purpose. Vendor shall implement measures to ensure that the source code is protected from unauthorized copy, use, duplication, modification, and is securely stored.

14.4. Vendor shall implement a change management process to include: tracking and formal approval of changes, back out procedures, and appropriate segregation of duties. All changes shall be tested

in a test environment and approved following a formal process prior to implementation to the production environment.

14.5. Vendor shall replace outdated and unsupported information systems and software of Vendor.

15. Logging and Monitoring

15.1. Vendor shall implement and maintain logging and monitoring measures in accordance with industry standards, Data Protection Laws, and the Agreement to (i) ensure the early detection of unusual, abnormal, unauthorized or malicious activities; and (ii) provide an audit trail of each system and transactional activity for subsequent review; and (iii) record all changes to Confidential Information and detail related to the access of Confidential Information. Unless otherwise required by law, Vendor shall retain its logs for a period of no less than six (6) months.

16. Audit, Inspection, and Accreditation

16.1. Vendor shall perform at least once every year or whenever there is a substantial change to Vendor's information systems, an audit of Vendor's information systems and organization that verifies compliance with its Security Policy and the Agreement. The audit shall be applied uniformly throughout Vendor's network to detect, investigate, and resolve all non-compliances.

16.2. Upon Entrust's request, Vendor shall permit Entrust (or a third party under the instruction of Entrust) to perform an audit of Vendor's and its Third Parties' information security program. Entrust or its appointed third party shall be allowed to carry out this audit not more than once a year, except in the event of a Data Security Breach, in which case Entrust may be permitted to conduct an additional audit. An audit will include the following conditions: (i) any audit will be limited in duration to five (5) business days, (ii) each party shall bear their own costs of an audit, (iii) the results of the audit shall remain confidential, (iv) and the audit will be non-invasive (e.g. no penetration testing, security scanning, etc.).

16.3. Entrust will detail any findings of an audit conducted under this Section 16 (Audit, Inspection, and Accreditation) and provide a report of those findings to Vendor. Vendor shall work toward addressing those findings in a timely manner. If Vendor fails to appropriately address Entrust's findings, Entrust shall have the right to terminate the Agreement.

16.4. Vendor shall hold and continuously maintain a third-party security certification, such as ISO 27001, SOC2 Type II, PCI-DSS, or other similar assessment, the scope of which shall cover the services delivered to Entrust. Upon request and at no additional charge to Entrust, Vendor shall provide a copy or evidence of its security certification.

17. Data Return and Destruction

17.1. Upon Entrust's request, termination or expiration of the Agreement, or Confidential Information is no longer needed for the purpose of performance under the Agreement, Vendor shall promptly return or destroy Entrust's data according to industry recognized standards such as NISTSP 800-88, DoD 5220-22M, or SEAP 8100/8200. Upon request, Vendor shall provide certification of destruction in accordance with this section.

17.2. Vendor shall strip all devices that contain storage media, such as laptops, smartphones, USB sticks, or other removable storage devices before throwing away or re-using the device.