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-

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 eep (2c)1.19(an)2-np aneyt1.19(an E2-5-5.5n)(p)5.2taTw 0 -1nptupSp53 (.Tw 03 T)28f i e (2c)1.19(an)2-n (4(tc)-3 (t

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 security@entrust.com. In Vendor's notice, Vendor shall specify to the extent available:

4.1.1.

cryptosystems currently in use (a “PQC Plan”). To the extent Vendor stores any Entrust Confidential Information, Vendor’s PQC Plan shall address the threat of “harvest now, decrypt later” programs. Upon request, Vendor shall provide an executive summary of its PQC plan.

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:

Vaic 68BDC(lu)2.2 (d)2.3 (in.6 (e[V).6 (e3)-1 (nt3 (a /P (e)- (al)10.5 (u)2.2 (s)-1.3 (e)-T-J0.04 Tw T[le)-3 (g)2.6 (it)0 Tc 9(an)2.3l h
V g i d (n) 2 . 3 r 9 (e) - 3 (s) - 1 . 4 l l o V e r
3 e 3 e 4 T w 4 3 e i 1 4 3 1 - 3 e c ((e) 5 . 6 [(3 e) -
V a i c 6 8 > > B D C (l u) P h a 9 (c) 8 . 9 (e) - 3
V a i c 6 8 > > B D C (l u) T [( ) 8 1 3 (- g) 8 e 3 e i

V a i c 6 8 > > B D C (l u) P h a 9 (c) 8 . 9 (e) - 3

9.8.

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 computT0 TcstT(,.772 0 Td( )Tj(s)12.5 (tC -

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,