Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. **Information Security Program.** Entrust maintains a comprehensive, written Information Security Management Program ("ISMP") that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope, and type of Entrust's business; (b) resources available; (c) the type and sensitivity of information that Entrust stores and processes; and (d) the need for security and protection from unauthorized disclosure of customer information. Entrust conducts periodic reviews of its ISMP and updates its ISMP as necessary to respond to evolving risks and industry standards.

Entrust's ISMP includes the following measures:

2. **Organization of Information Security**. Entrust's Chief Information Security Officer (CISO) oversees and is accountable for the success of the ISMP. Entrust employs a dedicated information security department that is appropriately staffed with skilled, knowledgeable, and well-trained personnel that are responsible for the execution of the ISMP.

3. **Physical and Environment Security.** Entrust ensures that its processing facilities, or any third-party data processing facilities that it utilizes, are maintained in physically and environmentally secure facilities that are designed to restrict unauthorized access or damage to Entrust's information data, assets and technology. These secure facilities include controls such as video surveillance cameras, alarm systems, badge and locked doors at entry points, walls extended from floor to ceiling, environmental detection and suppression mechanisms, backup power systems, and other appropriate and applicable physical and environmental security controls.

4. **Network and Systems Access.** Entrust maintains system access controls and policies to ensure only authorized users are permitted access to Entrust's network and systems. Such user access controls include (i) restricting user access based on least privileged principles, (ii) secure password or authentication requirements, (iii) multi-factor authentication where appropriate and applicable, (iv) timely revocation of access privileges, and (v) implementation of industry standard firewalls.

5. **Human Resources.** To the extent permitted by law, Entrust conducts background checks on all personnel prior to employment. Entrust maintains a security awareness training program that is reviewed and updated at least on an annual basis. The security awareness program focuses on the primary goal of protecting confidentiality, integrity, and availability of information in all forms. All Entrust personnel are required to read and attest to Entrust's information security policies on an annual basis.

6. **Incident Response.** Entrust maintains incident management plans and processes for addressing privacy and security incidents, including escalation paths to senior management, collection of evidence, forensics analysis as required, communication to

internal and external entities on a need-to-know basis, containment of the incident, remediation, and post-incident analysis to determine root cause. All Entrust employees and contractors are required to promptly report any suspected privacy or security weaknesses or events to its security operations center.

7. **Cryptography.** Entrust maintains cryptographic controls appropriate to the level of sensitivity of the information based on data classification of the information to be protected and in accordance with industry standards.

8. **Software and Application Development.** Entrust maintains written secure development life cycle (SDLC) policies, standards, and processes to ensure the security and integrity of applications and systems and to prevent source code from unauthorized and untested alterations. Entrust secure code development processes are aligned with industry standards and guidelines, such as OWASP, SANS CWE Top 25, and CERT. Before publicly launching new services or significant feature updates, Entrust performs application security reviews designed to identify, mitigate, and remediate security risks. Additionally, Entrust maintains formal processes for the approval of changes, backout procedures, and appropriate segregation of duties.

9. **Vulnerability Management.** Entrust maintains a continuous vulnerability management program to ensure the timely identification and remediation of internal and external vulnerabilities and risks. This process is built on industry certified tools and procedures and is facilitated by competent and experienced professionals. Entrust regularly updates and patches hardware and software to minimize the risk of vulnerabilities.

10. **Third-Party Management.** Entrust maintains third-party management procedures to ensure appropriate due diligence is conducted on authorized third parties that may impact the security of Entrust's systems and information.

11. **Business Continuity.** Entrust maintains a business continuity program ("BCP") that is designed to prevent, mitigate the consequences of, prepare for, respond to, maintain continuity during, and recover from emergency incidents. The BCP is organized through various written policies, procedures, standards, and recovery plans to address these goals. Entrust shall regularly test its BCP to ensure that it is effective at recovery and resumption of critical services and functions.

12. **Compliance and Certifications.** Entrust maintains security compliance certifications where appropriate to the service offering, regulatory requirements, and industry standards. An overview of Entrust's security certifications can be found on its website, located here: https://www.entrust.com/legal-compliance/security.