IDVERIFACT DATA SECURITY PROGRAM

IDVerifact has implemented and shall maintain a commercially reasonable security program in accordance with industry best practices, which shall include technical and organizational measures to ensure an appropriate level of security for Customer Personal Data taking into account the risks presented by the processing, in particular from the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to Customer Personal Data, and the nature of the Customer Personal Data to be protected having regard to the commercially available technology and the cost of implementation. IDVerifact's security programshall include the following measures.

1. Security Program

a. ISO27001-based Information Security Management System (ISMS): IDVerifact shall maintain an ISMS risk-based security program to systematically manage and protect the organization's business information and the information of its customers and partners.

b. Security Governance Committee: IDVerifact shall maintain a security committee comprised of executive and senior leaders that oversee IDVerifact's security program. This committee shall meet monthly to review the operational status of the ISMS (including risks, threats, remediation actions, and other security-related issues) and drive continuous security improvement throughout the business.

c. Security incident response policy: IDVerifact shall maintain policies and procedures to (1) investigate and respond to security incidents, including procedures to assess the threat of relevant vulnerabilities or security incidents using defined incident classifications and categorizations and (2) establish remediation and mitigation actions for events, including artifact and evidence collection procedures and defined remediation steps.

d. Policy maintenance: All security and privacy-related policies shall be documented, reviewed, updated, and approved by management at least annually to ensure they remain consistent with legal and regulatory requirements, and industry standards.

e. Communication and commitment: Security and privacy policies and procedures shall be published and effectively communicated to all personnel and relevant subcontractors. Security shall be addressed at the highest levels of IDVerifact with executive management regularly discussing security issues and leading company-wide security initiatives.

2. Personnel Security

a. Background screening: Personnel who have access to Customer Personal Data or the equipment on which it is stored shall be subject to background screening (as allowed by local laws and regulations) that shall include verification of identity, right to work and academic degrees and a check of criminal records, sex offender registries and prohibited/denied party lists.

b. Confidentiality obligations: Personnel who have access to Customer Personal Data shall be subject to a binding contractual obligation with IDVerifact to keep the Customer Personal Data confidential.

c. Security awareness training: Personnel shall receive training upon hire and at least annually thereafter covering security best practices and privacy principles.

d. Code of conduct: IDVerifact shall maintain a code of business conduct policy and compliance program to ensure ethical behaviour and compliance with applicable laws and regulations.

3. Third-Party Security

a. Screening: IDVerifact shall maintain policies and procedures to ensure that all new suppliers, SaaS applications, IT software, and IT service solutions are subject to reasonable due

diligence to confirm their ability to meet corporate security and compliance requirements as well as business objectives.

b. Contractual obligations: IDVerifact shall ensure that contractual agreements with suppliers include confidentiality and privacy provisions as appropriate to protect IDVerifact's interests and to ensure IDVerifact can meet its security and privacy obligations to customers, partners, employees, regulators, and other stakeholders.

c. Monitoring: IDVerifact shall periodically review relevant third-party suppliers to ensure the supplier complies with contractual terms, including any security and availability requirements. The monitoring program shall review relevant suppliers at least annually (regardless of the length of contractual term) to confirm that the supplier/solution is still meeting IDVerifact's objectives and the supplier's performance, security, and compliance procedures are still appropriate given the type of access and classification of data being accessed, controls necessary to protect data, and applicable legal and regulatory requirements.

4. Physical Security

a. Corporate facility security: A facility security program shall be maintained that manages building entrances, CCTVs, and overall security of its offices, including a security perimeter (including barriers such as card controller entry gates or manned reception desks). All employees, contractors and visitors shall be required to wear identification badges that distinguish their respective roles.

b. SaaS Services data center security: IDVerifact leverages Infrastructure as a Service (IaaS) data centers for hosting the SaaS Services. IDVerifact assesses the security and compliance measures of the applicable data center providers, and ensures that the providers are required to follow industry best practices.

5. Solution Security

a. Software development life cycle (SDLC): IDVerifact shall maintain a software development life cycle policy that defines the process by which personnel create secure products and services and the activities that personnel must perform at various stages of development (requirements, design, implementation, verification, documentation, and delivery).

b. Secure development: Product management, development, test, and deployment teams shall follow secure application development policies and procedures that are aligned to industry-standard practices.

c. Vulnerability assessment: IDVerifact shall regularly conduct risk assessments, vulnerability scans and audits (including third-party penetration testing of the SaaS Services twice annually and software upon each new version release). Identified product solution issues shall be scored using the Common Vulnerability Scoring System (CVSS) risk-scoring methodology based on risk impact level and the likelihood and potential consequences of an issue occurring. Vulnerabilities will be remediated based on assessed risk. Upon request from Customer, IDVerifact shall provide information about the identified vulnerabilities and the measures taken to remediate or address any such vulnerabilities.

6. Operational Security

a. Access controls: IDVerifact shall maintain policies, procedures, and logical controls to establish access authorizations for employees and third parties to limit access to properly authorized personnel and to prevent unauthorized access. Such controls shall include:
   i. requiring unique user IDs to identify any user who accesses systems or data.
   ii. managing privileged access credentials in a privileged account management (PAM) system.
   iii. communicating passwords separately from user IDs.
   iv. ensuring that user passwords are (1) changed at regular intervals; (2) of sufficient length and complexity; (3) stored in an encrypted format; (4) subject to reuse limitations; and (5) not assigned to other users, even at a different time; and
   v. automatically locking out users' IDs when several erroneous passwords have been entered.

b. Least privilege: IDVerifact shall ensure that personnel only have access to systems and data as required for the performance of their roles; only authorized personnel have physical access to infrastructure and equipment; access to production resources for the SaaS Services is restricted to employees requiring access, and access rights are reviewed and certified at least annually to ensure access is appropriate.

c. Malware: IDVerifact shall utilize industry-standard measures to detect and remediate malware, viruses, ransomware, spyware, and other intentionally harmful programs that may be used to gain unauthorized access to information or systems.

d. Encryption: IDVerifact shall use industry-standard strong encryption methods to protect data in transit and at rest as appropriate to the sensitivity of the data and the risks associated with loss; all laptops and other removable media, including backup tapes, on which Customer Personal Data is stored shall be encrypted.

e. Business continuity and disaster recovery (BCDR): IDVerifact shall maintain formal BCDR plans that are regularly reviewed and updated to ensure IDVerifact's systems and services remain resilient in the event of a failure, including natural disasters or system failures.

f. Data backups: IDVerifact shall backup data and systems using alternative site storage available for restore in case of failure of the primary system. All backups shall use strong encryption in transit and at rest.

g. Change management: IDVerifact shall maintain change management policies and procedures to plan, test, schedule, communicate, and execute changes to IDVerifact's SaaS Services infrastructure, systems, networks, and applications.

h. Network security: IDVerifact shall implement industry standard technologies and controls to protect network security, including firewalls, intrusion prevention systems, monitoring, network segmentation, VPN and wireless security. Networks shall be designed and configured to restrict connections between trusted and untrusted networks, and network designs and controlsshall be reviewed at least annually.

i. Data segregation: IDVerifact shall implement logical controls, including logical separation, access controls and encryption, to segregate each Customer's Personal Information from other Customer and IDVerifact data in the SaaS Services. IDVerifact shall additionally ensure that production and non-production data and systems are separated.