Expel, Inc.

Data Processing Addendum

This Data Processing Addendum ("**DPA**") supplements the Expel, Inc. Terms and Conditions (or a similar Services Agreement duly authorized and agreed to) (the "**Agreement**") between Customer and its applicable Affiliates ("**Customer**") and **Expel, Inc**., a Delaware corporation and its applicable Affiliates ("**Expel**"). Any terms not defined in this DPA shall have the meaning set forth in the Agreement.

Customer enters into this DPA on behalf of itself and, to the extent required under Applicable Privacy Laws, in the name and on behalf of its Affiliates permitted to use the Services under the Agreement. This DPA shall be effective as of the effective date of the Agreement.

1. DEFINITIONS

1.1 **Affiliate**(**s**) shall be defined as set forth in the Agreement, for the avoidance of doubt. In the event it is not defined in the Agreement, **Affiliate(s)** means an entity that directly or indirectly Controls, is Controlled by or is under common Control with a Party to this DPA. "Control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" will be construed accordingly.

1.2 **Applicable Privacy Laws** means any data protection laws or regulations applicable to the processing of Customer Personal Data in a specific jurisdiction, including European Privacy Laws, the California Consumer Privacy Act of 2018 (the **"CCPA"**), and the California Privacy Rights Act (the **"CPRA"**) in each case, as updated, amended or replaced from time to time.

1.3 **Customer Personal Data** means any Personal Data that is processed on behalf of Customer by Expel in connection with the Agreement, as more particularly described in Exhibit A.

1.4 **Data Privacy Framework** means the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) operated by the US Department of Commerce; as may be amended, superseded or replaced.

1.5 **Data Privacy Framework Principles** means the Principles and Supplemental Principles contained in the Data Privacy Framework; as may be amended, superseded or replaced.

1.6 **European Privacy Laws** means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**GDPR**"); (ii) the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (collectively the "**UK Privacy Laws**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); and (v) the Swiss Federal Data Protection Act of 19 June 1992 or the revised Federal Act on Data Protection of 25 September 2020 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 31 August 2022) ("**Swiss FADP**"); in each case as may be amended or superseded from time to time.

1.7 **Personal Data** means information which is protected as "personal data", "personal information" or any substantially similar term under Applicable Privacy Laws.

1.8 **Restricted Transfer** means a transfer of Personal Data originating from the European Economic Area, United Kingdom or Switzerland to a country that does not provide an adequate level of protection within the meaning of applicable European Privacy Laws.

1.9 **Security Incident** means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data stored or otherwise processed by Expel in connection with the provision of the Services. Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

1.10 **Standard Contractual Clauses** or **SCCs** means: (i) where the GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where UK Privacy Laws apply the EU SCCs as modified by the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**").

1.11 **Sub-Processor** means any third party Processor (including any Affiliates of Expel) appointed by Expel to process any Customer Personal Data (but shall not include Expel employees, contractors or consultants).

1.12 The following terms (and any substantially similar terms under Applicable Privacy Laws) shall have the meanings and otherwise be interpreted in accordance with Applicable Privacy Laws: Controller, Processor, Data Subject, process(ing) and transfer.

2. ROLES AND SCOPE OF PROCESSING

2.1 **Scope of DPA.** The Parties agree that this DPA shall govern the processing of any Customer Personal Data by Expel as a Processor (or functionally equivalent role) on behalf of Customer in connection with the provision of the Services pursuant to the Agreement(s).

2.2 **Details of Processing and Roles of the Parties.** The details of processing under this DPA are set forth in **Exhibit 1 – Details of Processing**. The Parties agree that Customer is the Controller with respect to the processing of Customer Personal Data and Expel is the Processor under European Privacy Laws, and the Parties may be subject to similar designations in other jurisdictions.

2.3 **Compliance with Law.** Any processing by either Party of Personal Data under or in connection with the Agreement shall be performed in accordance with Applicable Privacy Laws.

2.4 **Expel Responsibilities.** Expel shall process Customer Personal Data solely as necessary to provide the Services to Customer and at all times in accordance with Customer's documented instructions , as provided in this DPA or as provided thereafter, in writing, by an authorized representative of Customer (collectively **"Instructions"**). Expel shall promptly notify Customer if it believes that an Instruction violates Applicable Privacy Laws and in such event, Expel shall not be obligated to undertake such processing until such time as Customer has updated its Instructions and Expel has determined that the incidence of non-compliance is resolved. Notwithstanding the foregoing, Expel is not responsible for monitoring Customer's compliance with Applicable Privacy Laws or determining if Customer's Instructions are compliant with such laws. Furthermore, Expel has no obligation to assess Customer Personal Data in order to identify information that is subject to specific legal requirements.

2.5 **Customer Responsibilities.** Customer shall ensure that the Instructions comply with Applicable Privacy Laws and that the processing of Customer Personal Data by Expel in accordance with the Instructions shall not cause Expel to be in breach of Applicable Privacy Laws.

3. SUB-PROCESSING AND PERSONNEL

3.1 **Authorized Subprocessors.** Customer agrees that Expel may engage Sub-processors to process Customer Personal Data on Customer's behalf. A list of approved Sub-Processors as of the date of this DPA is set forth at https://expel.com/notices/#subprocessors.

3.2 **Notice of New Subprocessor.** If Expel wishes to replace or appoint any new Sub-Processor, Expel shall provide at least fourteen (14) days prior written notice to Customer of the Sub-Processor change and associated details of processing, except that if Expel reasonably believes engaging a new Sub-Processor on an expedited basis is necessary to protect the confidentiality, integrity or availability of Customer Personal Data or avoid a material disruption to the Services, Expel will give such notice as soon as reasonably practicable. Updates to the Sub-Processor list will be posted in the Expel Trust Center and a notification will be sent via email to Customer. Customer will be provided with ten (10) days to review (**'Review Period'**). The parties agree that non-response by Customer during the Review Period will be taken as Customer's approval of that proposed Sub-Processor update. If Customer objects to a Sub-Processor proposed under this Section 3.2 on good faith data protection grounds, Expel shall provide Customer with reasonable alternative(s), if any, to such engagement, including without limitation, modification to the Services. If Expel cannot provide any such alternative(s), or if Customer, acting reasonably, does not agree to any such alternative(s), Customer may terminate the Agreement and this DPA and Expel shall provide Customer with a pro-rata refund for all fees paid by Customer for Services not yet received.

3.3 **Sub-Processor Obligations.** With respect to all Sub-Processors authorized under Section 3.1 or 3.2:

1. Expel is responsible and liable to Customer for any acts or omissions of a Sub-Processor that cause Expel to breach any of its obligations under this DPA.

2. Prior to such Sub-Processor processing Customer Personal Data, Expel shall enter into a written agreement with each Sub-Processor which (a) requires the Sub-Processor to process Customer Personal Data in accordance with Applicable Privacy Laws; and (b) is at a minimum, as protective of Customer Personal Data as this DPA.

4. INTERNATIONAL TRANSFERS

4.1 **Location of Processing.** Expel may process Customer Personal Data in, or transfer Customer Personal Data to, any region in which Expel, its Affiliates and authorized Sub-Processors maintain facilities to perform the Services. Expel shall not process or transfer (directly or via onward transfer) Customer Personal Data (nor permit such data to be processed or transferred) outside of its country of origin unless it first takes such measures as are necessary to ensure the transfer is in compliance with Applicable Privacy Laws.

4.2 **European Data Transfers.** Where the transfer of Customer Personal Data between the Parties involves a Restricted Transfer and European Privacy Laws require that appropriate safeguards are put in place, the Parties agree that:

1. Expel participates in and certifies compliance to the Data Privacy Framework. Where and to the extent the Data Privacy Framework applies to the Restricted Transfer, Expel will (i) provide at least the same level of protection to Customer Personal Data required by the Data Privacy Framework Principles, and (ii) inform Customer if Expel determines that it is unable to comply with this requirement.

2. The Standard Contractual Clauses will be incorporated by reference and apply to the Restricted Transfer as follows:

a. In relation to transfers of Customer Personal Data subject to the GDPR, the EU SCCs will apply, completed as follows:

   i. Module 2 (Controller to Processor) will apply;

   ii. in Clause 7, the optional docking clause will not apply.

   iii. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes will be as set forth in Section 3.2 of this DPA.

   iv. in Clause 11, the optional language is excluded.

   v. in Clause 17, Option 1 will apply and the governing law shall be the laws of Ireland;

   vi. in Clause 18(b), disputes shall be resolved in the courts of Ireland;

   vii. the competent supervisory authority shall be the Irish Data Protection Commission; and

   viii. the remaining information required by the Annexes to the SCCs is set forth in the Exhibits to this DPA.

b. In relation to transfers of Customer Personal Data subject to UK Privacy Laws, the EU SCCs: (i) will apply as completed in accordance with paragraph (a) above; and (ii) shall be deemed amended as specified by the UK Addendum, which shall be deemed executed by the parties and incorporated into and form an integral part of this DPA. In addition, Tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Exhibits 1 and 2 of this DPA and Table 4 in Part 1 shall be deemed completed by selecting "neither party".

c. In relation to transfers of Customer Personal Data subject to the Swiss FADP, the EU SCCs will also apply in accordance with paragraph (a) above, with the following modifications:

   i. The supervisory authority with respect to such Personal Data is the Swiss Federal Data Protection and Information Commissioner.

   ii. References to "EU", "Union", a “Member State” and "Member State law" shall be replaced with Switzerland or "Swiss law".

   iii. Data Subjects located in Switzerland shall be able to enforce their rights in Switzerland.

   iv. References to the EU GDPR shall be understood to refer to the Swiss FADP (as amended or replaced).

   v. In Clause 17, Option 1 and the law of Switzerland will apply.

   vi. In Clause 18(b), disputes will be resolved in the courts of Switzerland.

   vii. References to the “competent supervisory authority” and “competent courts” shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner and competent courts in Switzerland.

3. If and to the extent that a court of competent jurisdiction or supervisory authority with binding authority orders (for whatever reason) that the measures described in this DPA

cannot be relied on to lawfully transfer Customer Personal Data from Customer to Expel, the Parties will reasonably cooperate to agree and take any actions that may be required to implement any additional measures or alternative transfer mechanism to enable the lawful transfer of Customer Personal Data.

5. SECURITY AND SECURITY INCIDENTS

5.1 **Confidentiality.** Expel shall ensure that all Customer Personal Data is treated as "Confidential Information" as defined in the Agreement.

5.2 **Data Retention.** Confidential Information, including Customer Personal Data, shall be returned or destroyed as set forth in the Agreement. The parties agree that the certification of deletion described in Clauses 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by Expel to Customer only upon Customer's written request.

5.3 **Technical and Organizational Security Measures.** Expel represents and warrants that it has implemented and will maintain appropriate technical and organizational security measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of Customer Personal Data in accordance with Applicable Privacy Laws, and that such measures shall include, but not be limited to, those security measures set forth in **Exhibit 2** ("**Security Measures**"). Customer acknowledges that the Security Measures are subject to technical progress and development and that Expel may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish overall security of the Services.

5.4 **Security Incident Response.** Expel shall, without undue delay (and in any event within seventy-two (72) hours) after becoming aware of a Security Incident, notify Customer of the Security Incident and, provide timely information relating to the Security Incident including the type of data affected and the identity of the affected person(s) as it becomes known or when reasonably requested by Customer. In the event of a Security Incident, Expel shall take such measures and actions as are appropriate to investigate, remedy or mitigate the effects of the Security Incident and shall keep Customer up-to-date about all material developments in connection with the Security Incident.

5.5 **Disclosure of Security Incident.** Insofar as it relates to or may be associated with Customer or any Customer Personal Data, the content and provision of any notification, public/regulatory communication or press release concerning the Security Incident shall be solely at Customer's discretion, except as otherwise required by applicable laws; provided Customer may not name Expel or otherwise reference Expel without Expel's prior written approval.

6. COOPERATION AND AUDITS

6.1 **Data Subject Rights and Cooperation.** Expel shall provide Customer with reasonable and timely cooperation to enable Customer to respond to and fulfil any requests, complaints or other communications from Data Subjects and regulatory or judicial bodies relating to the processing of Customer Personal Data under the Agreement, including requests from Data Subjects seeking to exercise their rights under Applicable Privacy Laws. In the event that any such request, complaint or communication is made directly to Expel, Expel shall promptly pass this on to Customer and shall not respond to such communication without Customer's express authorization (unless otherwise required by law, including to verify Expel's obligations with respect to such request). Unless otherwise required by law, Customer shall be solely responsible for correcting, amending or deleting any Customer Personal Data in accordance with Data Subject requests.

6.2 **Data Protection Impact Assessments**. To the extent required by Applicable Privacy Laws, and upon reasonable request, Expel will, considering the nature of the processing and the information available to Expel, provide Customer with reasonable cooperation and assistance to carry out

data protection impact assessments or consult with applicable data protection authorities related to its use of the Services.

6.3 **Audits and Security Certifications.** Expel shall maintain records in accordance with its SOC-2 framework and statements and ISO 27001, or similar Information Security Management System (**"ISMS"**) standards. Upon reasonable request and notice, Expel shall provide copies of relevant external ISMS certifications, audit report summaries and/or other documentation reasonably required by Customer to verify Expel's compliance with this DPA. Customer acknowledges and agrees that it shall exercise its audit rights under this DPA (including this Section 6.3 and where applicable, the Standard Contractual Clauses) by instructing Expel to comply with the audit measures described in Section 6.4 below.

6.4 **Onsite Audits.** While it is the parties' intention to ordinarily rely on Expel's obligations set forth in Section 6.3 to verify Expel's compliance with this DPA, following a Security Incident impacting Customer or following instruction from a data protection authority, Customer (or its appointed representatives) may carry out an inspection of Expel's data processing operations and facilities during normal business hours and subject to thirty days' (30) prior written notice.

7. Additional Provisions for California Personal Information

7.1 **Scope of Section 7.** This Section 7 (Additional Provisions for California Personal Information) shall apply only with respect to Expel's processing of Personal Data subject to Applicable Privacy Laws in California ("**California Personal Information**").

7.2 **Roles of the Parties.** When Processing California Personal Information in accordance with Customer's Instructions, the parties acknowledge and agree that Customer is a Business and Expel is a Service Provider for the purposes of the CCPA.

7.3 **Responsibilities.** The parties agree that Expel will process California Personal Information as a Service Provider strictly for the purpose of performing its obligations under the Agreement (the **"Business Purpose"**). The Parties agree that Expel shall not: (a) sell or share California Personal Information (as defined in the CCPA); (b) retain, use, or disclose California Personal Information for a commercial purpose other than for the Business Purpose or as otherwise permitted by the CCPA; or (c) retain, use, or disclose California Personal Information outside of the direct business relationship between Customer and Expel. Expel certifies that it understands and will comply with the restrictions set out in this Section 7.3 (Responsibilities).

8. MISCELLANEOUS

8.1 For the avoidance of doubt, any claim or remedies that Customer may have against Expel (including Expel's personnel) arising under or in connection with this DPA, including: (i) for breach of this DPA (including, where applicable, the Standard Contractual Clauses); (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer in connection with the subject matter of this DPA; or (iii) under Applicable Privacy Laws, including any claims relating to damages paid to a Data Subject, except to the extent prohibited by Applicable Privacy Laws, shall be subject to any exclusion of damages or limitation of liability provisions (including any agreed upon aggregate financial caps) that may apply under the Agreement. Any claims against Expel or its Affiliates under or in connection with this DPA (including, where applicable, the Standard Contractual Clauses) shall be brought solely by the Customer entity that is party to the Agreement. Notwithstanding any other provision of the Agreement or this DPA, in no event does this DPA restrict or limit the rights of any Data Subject under Applicable Privacy Laws.

8.2 The obligations placed upon Expel under this DPA shall survive so long as Expel and/or its Sub-Processors process Customer Personal Data on behalf of Customer in connection with the Agreement.

8.3 Except as set out in this DPA, the provisions of the Agreement shall remain unchanged and shall continue in force. In the event of any conflict between this DPA and any provisions set out in any Agreements, the parties agree that the terms of this DPA shall prevail.

8.4 No variation of this DPA shall be valid unless it is in writing (which excludes email) and signed by or on behalf of each of the parties by their respective authorised representatives.

8.5 No single or partial exercise, or failure or delay in exercising any right, power or remedy by any party shall constitute a waiver by that party of, or impair or preclude any further exercise of, that or any right, power or remedy arising under this DPA or otherwise.

8.6 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless otherwise required by Applicable Privacy Laws.

Exhibit 1

DETAILS OF PROCESSING

A. LIST OF PARTIES

Data exporter(s): The party identified as the "Customer" in the Agreement.

Activities relevant to the data transferred under these Clauses: Managed Detection and Response Services – provision of the Services by Data Importer on behalf of the Data Exporter as further described in the Agreement.

Role (controller/processor): Controller

Data importer(s):

Name: Expel, Inc.

Address: 12950 Worldgate Dr, Suite 200 Herndon, VA 20170 USA

Contact person's name, position and contact details:

Greg Notch, Chief Security Officer and Data Protection Officer

email: privacy@expel.com

Activities relevant to the data transferred under these Clauses: Managed Detection and Response Services – provision of the Services by Data Importer on behalf of the Data Exporter as further described in the Agreement.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

X Customers' customers / end-users of a Customer product or service

X Customer employees and/or staff

Categories of Personal Data transferred

X Other (list here):

- Email address
- IP address
- Geolocation
- Device/asset identifiers
- Customer system username
- Host name
- Full name (associated with an IP address)

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A – No sensitive data is transferred or otherwise processed under the Agreement.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Transfers occur on a continuous basis

Nature of the processing

The nature and purposes of processing carried out by the Data Importer on behalf of the Data Exporter shall be as set out in the Agreement, and may include any or all of the following purposes:

Provision of Managed Detection and Response Services

Purpose(s) of the data transfer and further processing

The nature and purposes of processing carried out by Expel on behalf of Customer shall be as set out in the Agreement, and may include any or all of the following purposes:

Provision of Managed Detection and Response Services

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Expel will retain Customer Personal Data in accordance with the retention periods described in Section 5.2 (Data Retention) of the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The nature and purposes of transfers to Sub-Processors are carried out by Expel on behalf of Customer shall be as set out in the Agreement, and may include any or all of the following purposes:

Managed Detection and Response Services

Exhibit 2

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Expel has implemented and shall maintain an information security program in accordance with its SOC-2 framework and ISO 27001.

This is an overview of some of the technical and organizational security measures that Expel implements to safeguard Customer Personal Data. Some solutions may have alternate safeguards outlined in the applicable Sales Order or other contracts as agreed with Customer or the applicable Customer Affiliate.

Security Practices

Expel has implemented corporate information security practices and standards that are designed to safeguard Expel's environments and to address business objectives across the following areas:

(1) information security

(2) system and asset management

(3) development, and

(4) governance.

These practices and standards have been approved by Expel's executive management and are periodically reviewed and updated where necessary.

Expel shall maintain an appropriate data privacy and information security program, including policies and procedures for physical and logical access restrictions, data classification, access rights, credentialing programs, record retention, data privacy, information security and the treatment of personal data and sensitive personal data throughout its lifecycle. Key policies should be reviewed at least annually.

Organizational Security

It is the responsibility of the individuals across Expel's organization to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, Expel's Information Security (**"IS"**) function is responsible for the following activities:

1. **Security strategy** – the IS function drives Expel's security direction. The IS function works to ensure compliance with security related policies, standards and regulations, and to raise awareness and provide education to users. The IS function also carries out risk assessments and risk management activities, and manages contract security requirements.

2. **Security engineering** – the IS function manages testing, design and implementation of security solutions to enable adoption of security controls across the environment.

3. **Security operations** – the IS function manages support of implemented security solutions, monitors and scans the environment and assets, and manages incident response.

4. **Forensic investigations** – the IS function works with Security Operations, Legal, Privacy, and Human Resources to carry out investigations, including eDiscovery and eForensics.

5. **Security consulting and testing** – the IS function works with software developers on developing security best practices, consults on application development and architecture for software projects, and carries out assurance testing.

Asset Classification and Control

Expel's practice is to track and manage key information and physical, software and logical assets. Examples of the assets that Expel might track include:

- information assets, such as identified databases, disaster recovery plans, business continuity plans, data classification, backups/backup operations, data retention requirements, and archived information
- software assets, such as identified applications and system software
- physical assets – desktops/laptops, printers, and communications equipment.

The assets are classified based on business criticality to determine confidentiality requirements. Industry guidance for handling personal data provides the framework for technical, organizational and physical safeguards. These safeguards may include controls such as access management, encryption, logging and monitoring, and data destruction.

Employee Screening, Training and Security

1. **Screening/background checks:** As part of the employment/recruitment process, Expel shall perform or have performed screening/background checks on employees (which shall vary from country to country based on local laws and regulations), and on employees of subcontractors where such employees will have access to Expel's networks, systems or facilities.

2. **Identification:** Expel shall require all employees to provide proof of identification and any additional documentation that may be required based on the country of hire or if required by other Expel entities or customers for whom the employee is providing services.

3. **Training:** Expel's compliance training program includes a requirement for employees and contractors to complete information security and privacy awareness training when they onboard at Expel followed by continuous security and privacy awareness videos that are watched by all employees and contractors on a monthly basis. The security and privacy awareness trainings provided by Expel may also provide materials specific to certain job functions.

4. **Confidentiality:** Expel shall ensure its employees are legally bound to protect and maintain the confidentiality of any personal data they handle pursuant to standard agreements.

Physical Access Controls and Environmental Security

1. **Physical Security Program:** Expel shall use a number of technological and operational approaches in its physical security program to mitigate security risks to the extent reasonably possible. Expel's security team works closely with each site to determine appropriate measures are in place to prevent unauthorized persons from gaining access to systems within which confidential information (including personal data) is processed and continually monitor any changes to the infrastructure, business and known threats. They also monitor best practice measures used by others in the industry and carefully select approaches that meet both uniqueness in business practice and expectations of Expel. Expel balances its approach towards security by considering elements of control that include architecture, operations and systems.

2. **Physical Access controls:** Physical access controls/security measures at Expel's facilities/premises are designed to meet the following requirements:

    a. access to Expel's buildings, facilities and other physical premises shall be controlled and based upon business necessity, sensitivity of assets and the individual's role and relationship to Expel. Only personnel associated with Expel are provided access to

Expel's facilities and physical resources in a manner consistent with their role and responsibilities in the organization;

b. relevant Expel facilities are secured by an access control system. Access to such facilities is granted with an activated card only;

c. all persons requiring access to facilities and/or resources are issued with appropriate and unique physical access credentials (e.g. a badge or key card assigned to one individual) by the IS function. Individuals issued with unique physical access credentials are instructed not to allow or enable other individuals to access Expel's facilities or resources using their unique credentials (e.g. no "tailgating"). Unique credentials are non-transferable and if an individual cannot produce their credentials upon request, they may be denied entry to Expel's facilities or escorted off the premises. At staffed entrances, individuals are required to present a valid photo identification or valid credentials to the security representative upon entering. Individuals who have lost or misplaced their credentials or other identification are required to enter through a staffed entrance and be issued a temporary badge by a security representative;

d. employees are regularly trained and reminded to always carry their credentials, store their laptops, portable devices and documents in a secure location (especially while traveling) and log out or shut down their computers when away from their desk;

e. visitors who require access to Expel's facilities must enter through a staffed and/or main facility entrance. Visitors must register their date and time of arrival, time of leaving the building and the name of the person they are visiting. Visitors must produce a current, government issued form of identification to validate their identity. To prevent access to, or disclosure of, company proprietary information visitors are not allowed un-escorted access to restricted or controlled areas;

f. select Expel facilities use CCTV monitoring, security guards and other physical measures where appropriate and legally permitted;

g. locked shred bins are provided on most sites to enable secure destruction of confidential information/personal data;

h. for Expel's major data centres, security guards, UPS and generators, and change control standards are available;

i. for software development and infrastructure deployment projects, the IS function uses a risk evaluation process and a data classification program to manage risk arising from such activities.

Change Management

The IT organization manages changes to the corporate infrastructure, systems and applications through a centralized change management program, which may include testing, business impact analysis and management approval where appropriate. All relevant application and systems developments adhere to an approved change management process.

Security Incidents and Response Plan

1. **Security incident response plan:** Expel maintains a security incident response policy and related plan and procedures which address the measures that Expel will take in the event of loss of control, theft, unauthorized disclosure, unauthorized access, or unauthorized use or acquisition of personal data. These measures may include incident analysis, containment, response, remediation, reporting and the return to normal operations.

2. **Response controls:** Controls are in place to protect against, and support the detection of, malicious use of assets and malicious software and to report potential incidents to Expel's IS function or Service Desk for appropriate action. Controls may include, but are not limited to: information security policies and standards; restricted access; designated development and test environments; virus detection on servers, desktop and notebooks; virus email attachment scanning; system compliance scans; intrusion prevention monitoring and response; firewall rules; logging and alerting on key events; information handling procedures based on data type; e-commerce application and network security; and system and application vulnerability scanning. Additional controls may be implemented based on risk.

Data Transmission Control and Encryption

Expel shall, to the extent it has control over any electronic transmission, transfer or storage of personal data, take all reasonable steps to ensure that such data cannot be read, copied, altered or removed without proper authority during its transmission, transfer or storage. In particular, Expel shall:

1. implement industry-standard encryption practices in its transmission and storage of personal data. Industry-standard encryption methods used by Expel includes Secure Sockets Layer (SSL), Transport Layer Security (TLS), a secure shell program such as SSH, and/or Internet Protocol Security (IPSec), and at least AES-256-bit encryption;

2. if technically feasible, encrypt all personal data, including, in particular any sensitive personal data or confidential information, when transmitting or transferring that data over any public network, or over any network not owned and maintained by Expel. Expel's policy recognizes that encryption is ineffective unless the encryption key is inaccessible to unauthorized individuals and instructs personnel never to provide an encryption key via the same channel as the encrypted document;

3. for Internet-facing applications that may handle sensitive personal data and/or provide real-time integration with systems on a network that contains such information (including Expel's core network), a Web Application Firewall (WAF) may be used to provide an additional layer of input checking and attack mitigation. The WAF will be configured to mitigate potential vulnerabilities such as injection attacks, buffer overflows, cookie manipulation and other common attack methods.

System Access Controls

Access to Expel's systems is restricted to authorized users. Access is granted based on formal procedures designed to ensure appropriate approvals are granted so as to prevent access from unauthorised individuals. Such procedures include:

1. **admission controls** (i.e. measures to prevent unauthorized persons from using data processing systems):

    a. access is provided based on segregation of duties and least privileges in order to reduce the risk of misuse, intention or otherwise;

    b. access to IT systems will be granted only when a user is registered under a valid username and password;

    c. Expel has a password policy in place which requires strong passwords for user login to issued laptops, prohibits the sharing of passwords, prohibits the use of passwords that are also used for non-work functions, and advises users on what to do in the event their password or other login credentials are lost, stolen or compromised;

    d. use of multifactor authentication ;

e. automatic computer lock, renewed access to the PC only after new registration with a valid username and password;

f. data and user classification determine the type of authentication that must be used by each system;

g. remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place as well as user authentication.

2. **Access controls** (i.e. measures to prevent unauthorised access to systems):

a. access authorization is issued in respect of the specific area of work the individual is assigned to (i.e. work role);

b. adjustment of access authorizations in case of changes to the working area, or in case an employee's employment is terminated for any reason;

c. granting, removing and reviewing administrator privileges with the appropriate additional controls and only as needed to support the system(s) in question;

d. event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

Data Access Control

Expel applies the controls set out below regarding the access and use of personal data:

1. personnel are instructed to only use the minimum amount of personal data necessary in order to achieve Expel's relevant business purposes;

2. personnel are instructed not to read, copy, modify or remove personal data unless necessary in order to carry out their work duties;

3. third party use of personal data is governed through contractual terms and conditions between the third party and Expel which impose limits on the third party's use of personal data and restricts such use to what is necessary for the third party to provide services.

Separation Control

Where legally required, Expel will ensure that personal data collected for different purposes can be processed separately. Expel shall also ensure there is separation between test and production systems.

Job Control

Expel shall process personal data in accordance with the applicable services agreement between Expel and Customer and in accordance with the instructions of Customer. The following controls will be implemented by Expel:

1. personal data is processed only to the extent necessary for contractual performance;

2. personnel are subject to a written obligation of confidentiality;

3. diligent selection of (sub)processor and other service providers;

4. third party use of personal data is governed through contractual terms and conditions between the third party and Expel which impose limits on the third party's use of personal data and restricts such use to what is necessary for the third party to provide services;

5. clear instructions to (sub)processors on security measures for protecting privacy including the appropriate technical and organizational measures to safeguard the personal data to the same or higher level of protection as provided by Expel;

6. ongoing monitoring of (sub)processor's activities.

Availability Control

Expel protects personal data against accidental destruction or loss by following these controls:

1. personal data is retained in accordance with customer contract or, in its absence, Expel's record management policy and practices, as well as legal retention requirements;

2. hardcopy personal data is disposed of in a secure disposal bin or a crosscut shredder such that the information is no longer decipherable;

3. electronic personal data is given to Expel's IT Asset Management team for proper disposal;

4. appropriate technical measures are in place, including (without limitation): anti-virus software is installed on all systems; network protection is provided via firewall; network segmentation; user of content filter/proxies; interruption-free power supply; regular generation of back-ups; fire safety system; water protection systems where appropriate; emergency plans; and air-conditioned server rooms provided by Expel's cloud hosting services providers.

Data Input Control

Expel has, where appropriate, measures designed to check whether and by whom personal data have been input into data processing systems, or whether such data has been modified or removed. Access to relevant applications is recorded.

System Development and Maintenance

Publicly released third party vulnerabilities are reviewed for applicability in Expel environment. Based on risk to Expel's business and customers, there are predetermined timeframes for remediation. In addition, vulnerability scanning, and assessments are performed on new and key applications and the infrastructure based on risk. Code reviews and scanners are used in the development environment prior to production to proactively detect coding vulnerabilities based on risk. These processes enable proactive identification of vulnerabilities as well as compliance.

Compliance

The information security, legal, and privacy compliance departments work to identify regional laws and regulations that may be applicable to Expel. These requirements cover areas such as, intellectual property of Expel and its customers, software licenses, protection of employee and customer personal information, data protection and data handling procedures, trans-border data transmission, financial and operational procedures, regulatory export controls around technology, and forensic requirements.

Mechanisms such as the information security program, the executive privacy council, internal and external audits/assessments, internal and external legal counsel consultation, internal controls assessment, internal penetration testing and vulnerability assessments, contract management, security and privacy awareness training, security consulting, policy exception reviews and risk management combine to drive compliance with these requirements.

When Expel enters into a contractual relationship with a Sub-Processor, the technical and organizational measures agreed upon are no less protective than the technical and organizational measures agreed between Customer and Expel.