INFORMATION SECURITY TERMS

1. Introduction

This document describes the technical and organisational measures and processes that Service Provider shall, at minimum, implement and maintain in order to protect personal data against risks inherent in the processing and all unlawful forms of processing (including, but not limited to, accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed) (the "**Security Measures**"). Service Provider will take into account the risks involved in the processing, the nature of the personal data, and the nature, scope, context, and purposes for processing when assessing the necessary level of security. Service Provider will maintain any necessary records and documentation (including in electronic form) to evidence its compliance with these Security Measures. Service Provider may update or modify its technical and organisational measures and processes from time to time, provided that such updates and modifications do not fall below the standards set forth in this document and do not result in the degradation of the overall security of the processing activities.

2. Information Security Program and Attestations

Service Provider maintains an information security program that includes the adoption and enforcement of internal policies and procedures designed to: (i) satisfy these Security Measures, (ii) identify reasonably foreseeable security risks and unauthorized access to personal data, and (iii) minimize security risks, taking into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of processing, and the risk of varying likelihood and severity for the rights and freedom of natural persons.

3. System Security

3.1 Access Controls. Service Provider will implement and maintain the following access controls to prevent any unlawful form of processing and Data Breaches:

3.1.1 User IDs. Unique user identification credentials must be assigned to all individual users.

3.1.2 Access Removal. Procedures for timely access removal must be implemented and regularly assessed.

3.1.3 Least Privilege and Need-to-Know. The principles of least privilege and need-to-know must be implemented, followed, and regularly reviewed (e.g., regular account and access reviews).

3.1.4 Passwords. Passwords shall have minimum length and complexity requirements. Passwords may not consist of names, simple words, or user IDs, or reverse spellings. Passwords may not be reused.

3.1.5 Authentication. Authentication credentials must be protected by encryption during transmission. Remote administration access to personal data shall use two-factor authentication.

3.1.6 Sessions. Sessions must automatically terminate or a password-protected screensaver must be activated when individual user sessions are inactive for fifteen (15) minutes. Management systems such as jump stations or bastion hosts must time out sessions at regular intervals, not to exceed twelve (12) hours.

4. Scanning and Administration.

Service Provider shall use industry security resources (*e.g.*, National Vulnerability Database, CERT/CC Advisories) to monitor for security alerts. Service Provider shall receive security advisories from its third-party vendors where applicable. Internal and external facing systems must be regularly scanned with industry standard security vulnerability scanning software to identify security vulnerabilities.

4.1 Logs. Information Systems and applications must log security events. These logs must be monitored on a regular basis and provide sufficient details as required in an investigation of events. Logs will be maintained for as long as necessary to enable troubleshooting and forensic investigations, and in any event, for a minimum of twelve (12) months.

4.2 Patches. A patch management program must be maintained to ensure up-to-date security patches are appropriately applied to Information Systems.

4.3 Malware. Anti-malware controls must be implemented and signature-based tools must check for new updates at least daily.

4.4 Change Control. A formal, documented change control process must be implemented for Information Systems.

5. Network Security

Service Provider's Wi-Fi must be secured using secure encryption protocols. Firewalls must implement a default deny methodology. A DMZ must be implemented to separate backend systems from internet-facing systems. For internet-accessible applications, a three-tier architecture must separate database systems from web application servers. Any changes to the network must be sufficiently tested. An intrusion detection or prevention system must be implemented that covers network traffic to the Information Systems and any events and alerts that are generated must be regularly reviewed. Discovered vulnerabilities must be remediated in a timely fashion. Information Systems must have appropriate security hardening (*e.g.*, CIS benchmarks) applied before deployment and maintained thereafter.

6. **End-User Devices**

Laptops and desktops used by Service Provider's personnel that may come into contact with Expeditors Personal Data must have full-disk encryption.

7. **Information and Data Security**

7.1 Information Security Policy. Service Provider must document and implement an information security standard and or policy that is reviewed at least annually.

7.2 Encryption During Transfer and At Rest. Personal data (including backups) transferred over external networks and via physical media must be encrypted during transfers and when at rest.

7.3 Business Continuity. Service Provider must have a documented and implemented business continuity plan that is tested annually.

7.4 Backup and Recovery. Service Provider must have documented and implemented backup procedures as well as a disaster recovery plan that is tested annually.

7.5 Retention. Service Provider must have a documented and implemented data retention policy.

8. Incident Response

Service Provider must maintain a documented incident response plan that is tested annually.

9. **Audits or Assessments**

Service Provider will perform security audits or assessments at least annually and conduct internal reviews of their cybersecurity controls against the NIST CSF framework.

10. **Training**

Service Provider shall provide all personnel with information security and data privacy awareness training at least once per year.

11. **Physical Security**

A physical security program must be maintained in accordance with industry standards and best practices. Service Provider will only use secure data center facilities (secured using industry standards) to store personal data.

12. **Definitions**

12.1 *Data Breaches*. A verified breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

12.2 *Information Systems*. Information technology resources that transmit, process, handle, store, modify, or make available personal data.

12.3 *Personal Data; Processing*. These terms shall have the meaning assigned to them in applicable law.