Extended Security Warranty Schedule

Introduction

This Extended Security Warranty Schedule was last updated on 4 May 2021.

This Extended Security Warranty Schedule is not a standard warranty and applies only to Customers who have subscribed to the Extended Security Warranty in accordance with clause 16.3 of the Taxlab Terms of Use (http://www.taxlab.online/taxlab-terms/).

Taxlab may update and/or vary this Extended Security Warranty Schedule from time to time provided that if the changes materially degrade the overall security in the Subscription Services, Taxlab will provide Customer at least 30 days' prior written notice (including by email) of such changes.

Customer acknowledges that Taxlab is an ISO/IEC 27001:2013 certified organisation which complies with Information Security Management System (ISMS) requirements under the standard. If there is any inconsistency between Taxlab's obligations under clause 5 of the Agreement and ISO/IEC 27001:2013, the requirements under ISO/IEC 27001:2013 will prevail to the extent of any inconsistency.

1. Definitions and Interpretations

1.1. In this Extended Security Warranty Schedule, unless the context otherwise requires or it is specified otherwise:

Privileged User means a user who has been allocated powers within the Subscription Services which are significantly greater than those available to the majority of users.

Processing means any operation or set of operations performed upon Customer Data, whether or not by automatic means. This includes operations such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

Required Policies has the meaning of that term given in clause 15.1 of this Extended Security Warranty Schedule.

Risk Assessment means a planned activity undertaken to identify information security risks, evaluate their potential impact and likelihood, including their impact on individuals who are the subject of any Personal Data, and compare to established risk criteria for acceptance or remediation.

Sanitised means when data in a development or test environment is disguised by overwriting it with realistic looking, but false, data of a similar type (e.g., by masking or substitution techniques, etc.).

2. Policies for Information Security

2.1. Taxlab has a written information security policy that is:

(a) comprehensive, addressing the information security risks and controls identified through the Risk Assessment process, for each area of information security;

(b) reflects the requirements of applicable law, including data protection laws;

(c) approved by executive leadership;

(d) published and communicated to all employees and applicable third-party contractors; and

(e) reviewed at least annually and updated to address:

(i) relevant organisational changes;

(ii) contractual requirements owed to customers;

(iii) identified threats or risks to information assets; and

(iv) relevant changes in applicable laws and regulations.

2.2. Taxlab ensures that executive leadership maintains an Information Security Management System. Responsibilities include:

(a) maintaining the information security management system and any supplemental requirements; and \

(b) identifying accountability for the execution of information security activities.

3. Human Resource Security

3.1. Taxlab performs background verification checks on employees or third-party contractors that have access to Customer Data, in accordance with relevant laws, regulations, and ethical requirements for each individual at least upon initial hire (to the extent permitted by law). The level of verification is appropriate according to the role of the employee or third-party contractor, the sensitivity of the information to be accessed in the course of that person's role, and the risks that may arise from misuse of the information. The following checks are performed for each individual, to the extent permitted by law:

(a) identity verification;

(b) criminal history; and

(c) employment history.

3.2. Taxlab requires employees and third-party contractors with access to Customer Data to commit to written information security, confidentiality, and privacy responsibilities with respect to that information. These responsibilities are binding and survive termination or change of employment or engagement. Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of Customer Data.

3.3. Taxlab provides information security awareness training to employees and third-party contractors upon hire and at least annually thereafter. Such training:

(a) is updated to include changes in organisational policies and procedures;

(b) is relevant to trainee job functions;

(c) communicates the formal disciplinary process in effect when personnel commit an information security breach;

(d) includes specific data protection training for Personal Data; and

(e) includes phishing awareness, either by simulations or explicitly in an annual course.

4. Asset Management

4.1. Assets that store or process Customer Data are identified and included within an asset register. At a minimum, version, license, and ownership information, are included for each asset within the register. Information assets are classified according to asset value, criticality, sensitivity, and the risks resulting from unauthorised disclosure of the information. Procedures for labelling and handling information assets have been developed for each asset classification.

4.2. Taxlab keeps all Customer Data in the cloud, secured within established and accredited data centres using well protected applications and services and other recognised brands.

4.3. The risks around physical security of those selected data centres is covered by Taxlab’s supplier policies, with all data centre providers Taxlab uses separately holding their own ISO/IEC 27001:2013 certificate or other standards that are equal or better.

4.4. Customer acknowledges and agrees that Taxlab primarily uses the Microsoft Azure platform to deliver the Subscription Services which is subject to Microsoft's standard security and availability policies as updated from time to time by Microsoft (and available on its website). Customer data is stored in the Australia East and Australia Southeast regions. Should Taxlab plan a change to the platform, hosting provider or location of the servers used by Taxlab to deliver the Subscription Services, Taxlab agrees to provide Customer reasonable notice of such a change.

4.5. Taxlab has put in measures to protect against unattended sessions and equipment:

(a) System sessions automatically terminate or revalidate after a maximum of 5 minutes;

(b) Subscription Services sessions automatically terminate or revalidate after a maximum of 30 minutes; and

(c) Infrastructure containing Customer Data stored within Subscription Services are controlled by Microsoft Azure Active Directory Privileged Identity Management and access automatically expires 2 hours after it is granted.

Additionally, a clear desk and clear screen policy is enforced.

4.6. Taxlab Staff are not permitted to print any Customer sensitive information except to the extent necessary to test any printing and/or security features of

Taxlab's products. Such printing is then required to be shredded or securely destroyed.

4.7. Taxlab has controls to protect equipment, information, and assets located off-premise and/or during remote access sessions such as teleworking or remote administration. Teleworking, mobile device, and removable media policies are implemented and enforced.

4.8. Taxlab encrypts remote access communications to systems or applications containing Customer Data and requires a minimum of multi-factor authentication, virtual private networking device access or equivalent, and restricted ports and protocols.

4.9. Personally owned and managed equipment is not permitted to be used to access or store Customer Data. A bring your own device model is controlled by Taxlab and contains controls commensurate with those on corporate-owned devices.

4.10. Removable media devices (e.g. USB drives, memory sticks, Bluetooth storage devices) are disabled on all systems. Customer Data is not transferred using removable media devices. Other data is only transferred using removable media devices in one-off operations and only where approved in writing by executive leadership and data is encrypted and deleted immediately from the removable device after the operation has been completed.

4.11. Taxlab maintains procedures to ensure that Customer Data, is securely destroyed when no longer needed for the purposes authorised by the Customer or at the times set out and in accordance with the Agreement (i.e., following the expiration or termination of the Agreement). In particular:

(a) secure erasure of Customer Data is confirmed prior to asset destruction and disposal;

(b) Taxlab maintains records of destruction; and

(c) Taxlab requires any third parties engaged to process Customer Data to securely dispose of the information when no longer needed for the services they are required to deliver.

4.12. Where it is not possible to irretrievably destroy Customer Data held in electronic format, Taxlab takes reasonable steps to put the Customer Data beyond use.

4.13. Employees and third-party contractors agree to documented policies for the acceptable use and handling of assets. Assets are returned immediately upon termination of employment, and return of assets is tracked and verified.

4.14. Taxlab has formal, documented system hardening procedures and baseline configurations. Unsupported software or hardware are not used.

5. Access Control

5.1. Taxlab has formal, documented access control policies to support creation, amendment, and deletion of user accounts for systems or applications holding or allowing access to Customer Data. Taxlab has a formal, documented user account and access provisioning process to assign and revoke access rights to systems and applications. User account privileges are allocated on a "least privilege" basis and are formally authorised and documented. Taxlab prohibits the use of “generic” or “shared” accounts without system controls enabled to track specific user access and prevents shared passwords.

5.2. Privileged User access rights are:

(a) restricted to users with clear business need;

(b) assigned to a separate user account, to be used only for the time period required to complete the necessary task;

(c) segregated appropriately (e.g., code migration, security administration, audit log permissions, production support administration, etc.);

(d) captured by system logs and periodically reviewed; and

(e) accomplished by multi-factor authentication.

5.3. Taxlab monitors and restricts access to utilities capable of overriding system or application security controls. Administrator access rights to workstation endpoints are restricted. System and application owners review user access rights for appropriateness on a monthly basis. Inappropriate access is revoked immediately upon identification.

5.4. Taxlab use Microsoft Azure Active Directory Privileged Identity Management to control access requests to Customer Data. Access automatically expires two hours after it is granted. User access rights to systems and applications storing or allowing access to Customer Data are removed upon termination or change of employment responsibilities. Specifically, user access rights are:

(a) removed within 24 hours, upon termination of employment; and

(b) reviewed and adjusted within one week, upon change of employment responsibilities.

5.5. User access to systems and applications storing or allowing access to Customer Data is controlled by a secure logon procedure. To support this, Taxlab uses Microsoft Azure for password management. Taxlab also has the following controls for user authentication:

(a) each user account ID must be unique;

(b) each user account has a password;

(c) if set by system administrator, initial password issued is random and is changed by the user upon first use;

(d) users should set their own passwords as part of a password management system; and

(e) passwords are treated as confidential data and are encrypted upon transmission.

5.6. Taxlab supports single sign on or multi-factor authentication.

6. Cryptography

6.1. Customer Data, is encrypted at rest.

6.2. Taxlab uses Microsoft Azure Key Vault for key management. Taxlab has cryptographic key management procedures that include the following:

(a) generation of cryptographic keys with approved key lengths;

(b) secure distribution, activation and storage, recovery, and replacement/update of cryptographic keys;

(c) immediate revocation (deactivation) of cryptographic keys upon compromise or change in user employment responsibility;

(d) recovery of cryptographic keys that are lost, corrupted or have expired;

(e) backup and archive of cryptographic keys and maintenance of cryptographic key history;

(f) allocation of defined cryptographic key activation and deactivation dates;

(g) restriction of cryptographic key access to authorised individuals; and

(h) complying with local legal and regulatory requirements.

7. Physical and Environmental Security

7.1. Taxlab keeps the majority of information assets in the cloud, secured within established and accredited data centres using well protected applications and services and other recognised brands.

7.2. The risks around physical security of those selected data centres is covered by their supplier policies, with all data centre providers that Taxlab uses separately holding their own ISO/IEC 27001:2013 certificate or other standards that are equal or better.

8. Operations Security

8.1. Taxlab defines capacity requirements and monitors service availability.

9. Communications Security

9.1. External network perimeters are hardened and configured to prevent unauthorised traffic. Inbound and outbound points are protected by firewalls and intrusion detection systems. Ports and protocols are limited to those with specific business purpose. Web and application servers are separated from corresponding database servers by the use of firewalls.

9.2. Taxlab has access controls on wireless networks with strong encryption and strong authentication (e.g., WPA2) are used.

9.3. Taxlab relies in Microsoft Azure for synchronisation of system clocks on network servers to UTC (coordinated universal time).

9.4. Taxlab has internet filtering procedures to protect end user workstations from malicious websites and unauthorised file transfers outside the network.

9.5. Customer Data is encrypted during transmission across networks, including over untrusted networks (e.g., public networks) and when writing to removable devices. Taxlab uses platform and data-appropriate encryption. Certificates used for encryption in transit are obtained from an acknowledged certification authority.

9.6. Taxlab encrypts data during transmission between the Internet, the cloud environment, and the Customer network; between each application tier; and between interfacing applications. Cryptographic keys shall be supplied and governed by the Customer (e.g., creation, rotation, and revocation). Management and usage of cryptographic keys are segregated duties.

9.7. Taxlab uses Google Workspace for email and file storage systems used in the exchange of Customer Data and rely on Google's:

(a) commonly accepted security features, including anti-virus, file inspection, and filtering of known bad IP addresses;

(b) security configuration to protect against common email exploits, including spoofing, anonymous relay functionality, directory harvesting, and denial of service attacks;

(c) encryption method for web client connectivity to email systems; and

(d) encryption method for Customer Data in transit and at rest.

10. System Acquisition, Development and Maintenance

10.1. Taxlab performs penetration testing for the Subscription Services annually and when significant changes are made to the Subscription Services. Testing includes relevant Open Web Application Security Project Top 10 vulnerabilities. Any vulnerability identified during the testing which is defined as "critical" or "high" risk is addressed within 10 Business Days. All other vulnerabilities that do not fall within these categories are addressed within 30 days.

10.2. Upon request by the Customer, Taxlab may provide complete testing results, which include the number of critical, high, and medium severity findings; the name of the third party tester; and the date of such third-party testing.

10.3. Taxlab relies on Microsoft Azure Platform as a Service (PaaS) which has a patch and vulnerability management process to identify, report, and remediate system and application vulnerabilities by:

(a) performing vulnerability scans on a monthly basis and during any major system or application updates;

(b) implementing vendor patches or fixes; and

(c) developing procedures to address the remediation of identified vulnerabilities.

The procedures are approved by the application or system owner and by implemented commensurate with the level of risk.

10.4. Taxlab uses Microsoft Defender on all workstations and on our Azure environment we use PaaS which is managed by the Azure platform.

10.5. Taxlab generates administrator and event logs for systems and applications that store, allow access to, or process Customer Data. Logs are archived for a minimum of 180 days. Logs for all application, systems, or infrastructure that support, process, or store confidential or highly confidential Customer Data are archived for at least one year. Logs capture date, time, user ID, device accessed, and port used. Logs capture key security event types (e.g., critical files accessed, user accounts generated, multiple failed login attempts, events related to systems that have an Internet connection). Access to modify system logs are restricted. Logs can be provided to Customer upon request. Taxlab uses Azure Sentinel, which is a cloud-native security information and event manager platform with built in artificial intelligence, to review system logs in real time to identify system failures, faults, or potential security incidents affecting Customer Data. Corrective actions are taken to resolve or address issues within any required timeframes.

10.6. The hardware, software, and service procurement process is documented and includes identification and evaluation of information security risks.

10.7. Taxlab has formal, documented change control procedures to manage changes to information systems, supporting infrastructure, and facilities.

10.8. Taxlab logically or physically separate environments for development, testing, and production. User access to environments and Customer Data, is restricted and segregated, based on job responsibilities. User access to program source code is restricted and tracked.

10.9. Secure system engineering and coding practices have been established, documented, and integrated within the system development life cycle. Developers attend secure development training periodically.

10.10. Subscription Service changes undergo testing and meet defined acceptance criteria prior to implementation. Testing includes relevant security controls. Changes that have a major impact on Customer Data will be communicated to Customer with a minimum of 30 days’ notice prior to release.

10.11. Customer Data for use in a production environment will not be used within a test environment without written permission from the Customer and Taxlab executive leadership. If usage is approved, data will be masked (e.g. obfuscated, Sanitised, de-identified, Anonymised) or the non-production environment will have security controls equivalent to those within the production environment.

10.12. Source code undergoes automated static source code analysis and vulnerability remediation prior to implementation. Post-implementation testing shall occur subsequent to system changes, to validate that existing applications and security controls were not compromised.

10.13. Taxlab monitors outsourced system development activities, subject to third party supplier management controls.

11. Supplier Relationships

11.1. Supplier agreements with third parties processing Customer Data includes appropriate information security, confidentiality, and data protection requirements. Agreements with such parties are reviewed periodically to validate that information security and data protection requirements remain appropriate. Taxlab reviews its third parties' information security controls periodically and validates that these controls remain appropriate according to the risks represented by the third party's handling of Customer Data, taking into account technology needs and the costs of implementation.

11.2. Taxlab restricts third party access to Customer Data. When access to Customer Data is necessary for performance by third parties of the supplier agreements with those third parties, Taxlab will:

(a) provide the Customer with a list of third parties with required access to the Customer Data when requested by the Customer;

(b) permit access to Customer Data only as necessary so that the relevant third party can perform its obligations under the relevant supplier agreements; and

(c) record third party access to Customer Data within system logs, subject to Taxlab's controls for logging and monitoring.

12. Information Security Incident Management

12.1. Taxlab maintains a formally documented incident management policy that includes:

(a) clearly defined management and user roles and responsibilities;

(b) a reporting mechanism for suspected vulnerabilities and events affecting the security of Customer Data (including reporting of suspected unauthorised or unlawful access, disclosure, loss, alteration, and destruction of Customer Data);

(c) procedures for assessment of, classification of, and response to, security incidents within reasonable timeframes and proportionate to the nature of the security incident and the harm, or potential harm, caused;

(d) procedures for notification to relevant authorities as required by law, within the timeframes required by law;

(e) procedures for forensic investigation of a security incident; and

(f) a process for incident and resolution analysis designed to prevent the same, or similar, incidents from happening again.

12.2. Taxlab maintains a security incident tracking system that documents the following items for each security incident affecting Customer Data:

(a) incident type, including how and where the incident occurred;

(b) whether there has been any unauthorised or unlawful access, disclosure, loss, alteration or destruction of Customer Data;

(c) the Customer Data affected by the incident, including the categories of any Personal Data affected;

(d) the time when the incident occurred, or is estimated to have occurred; and

(e) remediation actions taken to prevent the same, or similar, incidents from happening again. Incident documentation is reviewed periodically to validate response and resolution.

12.3. If a security breach results in loss, destruction or damage to Customer Data, Taxlab will notify Customer within 24 hours after Taxlab becomes aware of the breach.

12.4. Taxlab supports any investigation (e.g., by the Customer, law enforcement, or regulatory authorities) that involves the Customer Data. Forensic procedures will be developed to support incident investigation. Engagement with a forensic specialist would be considered. Integrity of event and system log data shall be forensically maintained. Local legal requirements will be followed.

13. Information Security Aspects of Business Continuity Management

13.1. Taxlab performs business continuity risk assessment activities to determine relevant risks, threats, impacts, likelihood, and required controls and procedures. Based on risk assessment results, Taxlab documents, implements, annually tests and reviews business continuity and disaster recovery plans to validate the ability to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident that results in loss or corruption of Customer Data. Business continuity and disaster recovery plans include:

(a) availability requirements for Customer's services, specifying critical systems and agreed upon recovery points (RPO) and recovery time objectives (RTO);

(b) clearly defined roles and responsibilities;

(c) provisions for a geographically separate alternate site subject to physical and environmental controls; and

(d) backup and restoration procedures that include Sanitisation, disposal, or destruction of data stored at the alternate site.

For the provision of the Subscription Services, the target RPO is no more than 1 hour and the target RTO is no more than 4 hours.

13.2. Information backup procedures and media include:

(a) strong encryption technology;

(b) integrity validation;

(c) reconciliation with disaster recovery requirements; and

(d) secure offsite storage supporting availability requirements.

14. Compliance

14.1. Taxlab periodically reviews whether its systems and equipment storing, enabling access to, or otherwise processing Customer Data comply with legal and regulatory requirements and contractual obligations owed to the Customer. Upon request, Taxlab may allow the Customer to monitor and assess adherence to contractual requirements, including information security controls. Taxlab may also make relevant documentation, reports, and/or evidence available for review. All disclosed information is subject to the confidentiality obligations under clause 9 of the Agreement and all requests must be commercially reasonable.

14.2. Taxlab reviews the technical and organisational controls implemented to protect Customer Data for compliance with agreed-upon information security controls at least annually and the report results may be made available to the Customer upon request.

14.3. Taxlab maintains current independent verification of the effectiveness of its technical and organisational security measures, including ISO 27001 certification. The independent information security review is performed at least annually.

14.4. Taxlab complies with a documented termination or conclusion of service process. Non-disclosure and confidentiality responsibilities with respect to Customer Data remains in place following Agreement termination or conclusion. A primary point of contact will be identified to support the service termination process. Taxlab communicates agreement termination or conclusion to relevant employees and stakeholders. Taxlab revokes access to the Subscription Services promptly upon completion or termination of the Agreement.

15. Insurance

15.1. During the term of this Agreement, and for a period of six years thereafter in the case of policies written on a “claims made” basis, Taxlab maintains in force with a reputable and financially sound insurance company, at least the following insurance policies (**Required Policies**):

(a) public and products liability insurance in an amount of NZD$20 million in the aggregate; and

(b) professional indemnity insurance in an amount of NZD$5 million in the aggregate.

15.2. In addition to the Required Policies, Taxlab maintains in force with a reputable and financially sound insurance company workers’ compensation insurance in accordance with applicable legislation and/or awards.

15.3. Taxlab may provide Customer certificates of currency for the Required Policies upon written request.

15.4. If for any reason an insurer cancels, or fails or declines to renew, a Required Policy, then Taxlab will, at its own cost, as soon as reasonably practicable purchase a replacement policy and ensure that the replacement policy includes “prior acts coverage endorsement” effective from the date on which the previous Required Policy ceased to take effect.