Security Measures

Last updated: November 30, 2020.

These Software Compliance ('SWC") and ComplianceWare Security Measures ("Security Measures") are incorporated into and form part of your applicable agreement with SWC with respect to your use of ComplianceWare (the "Agreement") as deployed in the designated cloud provider platform/s (the 'Cloud Services'). The Security Measures set out the features, processes, and controls applicable to the Cloud Services which employ industry standard information security best practices.

1. Definitions

The following terms have the following meanings when used in the Security Measures. Any capitalised terms that are not defined in the Security Measures have the meaning provided in your Agreement.

1.1. "**Cloud Provider**" means Amazon Web Services (AWS), Microsoft Azure (Azure), or Google Cloud Platform (GCP), as selected by SWC.

1.2. "**Customer Data**" means any data you or your end users upload into the Cloud Services.

1.3. "**Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Data.

1.4. "**Security Measures**" means SWC's written security program, policies, and procedures that set forth the administrative, technical, and physical safeguards designed to protect Customer Data.

1.5. "**ComplianceWare Node**" means each data-bearing node containing the ComplianceWare file-store that is managed by ComplianceWare.

1.6. "**ComplianceWare Cluster**" means one or more associated ComplianceWare Clusters with a shared set of authorisation, network and database configurations.

1.7. "**SWC Systems**" means SWC's internal infrastructure, including development, testing, and production environments, for ComplianceWare.

1.8. "**Privileged User**" means a select SWC employee or third-party contractor who has been granted unique authority to access Customer Data or SWC Systems as required to perform his or her job function.

1.9. "**Security Incident Response**" means SWC's protocols for evaluating suspected security threats and responding to confirmed Data Breaches and other security incidents.

2. Information Security Overview.

2.1. General. SWC maintains its Security Measures to establish effective administrative, technical, and physical safeguards for Customer Data, and to identify, detect, protect against, respond to, and recover from security incidents. SWC's Security measures are designed in accordance with applicable data protection law.

2.2. Maintenance and Compliance. SWC's Security Measures are maintained by our Security Officer. SWC monitors compliance with its Security Measures and conducts ongoing education and training of personnel to ensure compliance. The Security Measures are reviewed and updated annually to reflect changes to our organisation, business practices, technology, services, and applicable laws and regulations. We will not alter or modify the Security Measures in a way that materially weakens or compromises the effectiveness of its security controls.

2.3. SWC Personnel Controls.

2.3.1. **Background Checks**. SWC performs industry standard background checks on all SWC employees as well as any third-party contractor with access to Customer Data or SWC Systems.

2.3.2. **Personnel Obligations**. Any Privileged User authorised to access Customer Data is required by the terms of their employment to information security and confidentiality obligations that survive termination and change of employment. SWC maintains a disciplinary procedure for violations by SWC personnel of its security policies and procedures.

2.3.3. **Training**. Upon hire and subsequently at each anniversary, Privileged Users authorised to access Customer Data undergo training on specific security topics, including phishing, protection of digital identities, network security, and the handling of Customer Data. In addition to these mandatory trainings, SWC offers employees additional training resources, such as web-based security reading groups and external experts and advisory groups.

2.4. Third Parties. SWC's evaluation and approval of third-party service providers prior to onboarding includes appropriate due diligence regarding each third-parties security processes and controls. We require third-parties to contractually commit to confidentiality, security responsibilities, security controls, data reporting obligations, and perform ongoing targeted due diligence on an annual basis.

2.5. Security Contact. If you have security concerns or questions, you may contact us via normal Support channels or by emailing security@swcompliance.com.au.

3. ComplianceWare Security Controls.

3.1. Data Centers and Physical Storage. ComplianceWare runs on AWS, Azure, and/or GCP as determined by SWC. Each Cloud Provider's data centers are compliant with a number of physical security and information security standards, which are detailed at the Cloud Provider's respective websites:

- https://aws.amazon.com/security/
- https://www.microsoft.com/en-us/trustcenter/security/azure-security
- https://cloud.google.com/security/

SWC selects the region ComplianceWare is to be hosted based on the designated geographic location that has applicable jurisdiction and in which the Customer Data primarily resides.

3.2. Encryption.

3.2.1. **Data in Transit**. All ComplianceWare network traffic is protected by Secure Sockets Layer (SSL/HTTPS), which is enabled by default and cannot be disabled. SSL certificates are obtained from a major, widely trusted third-party public certificate authority.

3.2.2. **Encryption at Rest**. Upon creation of a ComplianceWare Node, by default, Customer Data is encrypted at rest using AES-256 to secure all volume (disk) data. That process is automated by the transparent disk encryption of the selected Cloud Provider, and the Cloud Provider fully manages the encryption keys.

3.3. Network Connectivity Options.

3.3.1. **Network Isolation**. ComplianceWare is deployed in a shared multi-tenant system. Each such ComplianceWare Cluster utilises data model and programmatic practices to provide logical separation of your Customer Data.

3.3.2. **Host Whitelisting**. Inbound network access domain whitelisting is enabled to allow specific connections to ComplianceWare. Other network traffic is prevented from accessing your ComplianceWare Cluster.

3.4. Configuration Management. The ComplianceWare environment, including the ComplianceWare Clusters, leverages configuration management systems to fully automate configuration based on one-time decisions that are securely applied to new and existing environments to ensure consistency every time. ComplianceWare Clusters use in-house built images with secure configuration management applied via industry standard automation software, which includes hardening steps.

4. Access Controls.

4.1. Customer Access. ComplianceWare provides authentication and authorisation options for both the ComplianceWare UI and ComplianceWare Clusters.

4.1.1. **ComplianceWare UI Authentication and Authorisation**. User credentials for the ComplianceWare UI are stored using industry standard one-way hashes and allows you to define permissions for individual users or groups in order to restrict the Customer Data that is accessible in a query. Further, you may choose to assign each user a ComplianceWare-specific role, which authorises that user to perform specific actions in ComplianceWare. You can request changes to review, limit, or revoke user access at any time.

4.1.2. **Customer Database Auditing**. ComplianceWare offers granular auditing that monitors actions in ComplianceWare and is designed to detect any unauthorised access to Customer Data, including create, read, update, and delete (CRUD) operations and role-based access controls.

4.2. SWC Personnel Access to ComplianceWare Clusters.

4.2.1. **Privileged User Access**. As a general matter, SWC personnel do not have authorisation to access your ComplianceWare Clusters. Only a small group of Privileged Users are authorised to access your ComplianceWare Clusters in rare cases where required to investigate and/or restore critical services. SWC adheres to the principle of “least privilege” with respect to those Privileged Users, and any access is limited to the minimum time and extent necessary to repair the critical issue.

4.2.2. **Credential Requirements**. Privileged User accounts may only be used for privileged activities, and Privileged Users must use a separate account to perform non-privileged activities. Privileged User accounts may not use shared credentials. The password requirements described in Section 4.3.3 also apply to Privileged User accounts.

4.2.3. **Access Review and Auditing**. SWC reviews Privileged User access authorisation on a quarterly basis.

Additionally, we revoke a Privileged User's access when it is no longer needed, including within 24 hours of that Privileged User changing roles or leaving the company. We also log any access by SWC personnel to your ComplianceWare Clusters which include a timestamp, actor, action, and output.

4.3. SWC Personnel Access to SWC Systems.

4.3.1. **General**. SWC's policies and procedures regarding access to SWC Systems adhere to the principles of role-based access control (RBAC), least privilege, and separation of duties. In accordance with these principles, with respect to ComplianceWare, SWC developers are only granted access to our development environments, and access to our production environment is limited to Privileged Users with appropriate authorisations. We review access authorisations to SWC Systems on a quarterly basis. As part of the employee off-boarding process, access to SWC Systems is revoked within 24 hours of an employee's termination.

4.3.2. **Access to ComplianceWare Production Environment**. Our backend production environment that runs ComplianceWare is only accessible by a dedicated Privileged Users whose privileges must be approved by senior management.

4.3.3. **Credential Requirements.** All SWC personnel passwords must be at least eight characters, and can't be too similar to other personal information, a commonly used password, or entirely numeric. Passwords may not contain part of a username or the person's first or last name.

4.4. Physical Controls at SWC Offices. As noted in Section 3.1, Customer Data is hosted at the data centers of the selected Cloud Provider, and not at facilities owned or operated by SWC. At SWC offices, we follow industry best practices to employ physical security controls that are appropriate to the level of risk posed by the information stored and the nature of operations at our offices, which includes surveillance systems to monitor activity at points of entry from public spaces.

5. SWC Systems Security.

5.1. Separation of Production and Non-Production Environments. ComplianceWare has physical separation between production and non-production environments. Our non-production environments are utilized for development, testing, and staging.

5.2. Software Development Lifecycle. SWC develops new products and features in a multistage process using industry standard methodologies that include regular code reviews, documented policies and procedures for tracking and managing all changes to our code, source code commits, code versioning, IDE code analysis, and manual source code analysis.

5.3. Monitoring and Alerting. SWC monitors the health and performance of ComplianceWare without needing to access your ComplianceWare Clusters. SWC maintains a centralized log management system for the collection, storage, and analysis of log data for our ComplianceWare production environment and your ComplianceWare Clusters. We use this information for health monitoring, troubleshooting, and security purposes, including intrusion detection. We utilise a combination of automated alerting and human review to monitor the data.

5.4. Vulnerability Management.

5.4.1. **ComplianceWare Vulnerability Scanning**. SWC's vulnerability management policy requires individuals to

identify known vulnerabilities in system components and develop remediation timeframes commensurate to the severity of an identified issue. We also receive and monitor security bulletins for relevant software and libraries, and implement patches if security issues are discovered.

5.4.2. **Vulnerability Remediation**. SWC tracks all security issues until remediation. We implement patches to our system stack and applications on a need-to-update basis, Development tasks for all patches, bug fixes, and new features are defined as issues for specific target releases and are deployed to production after completing requisite checkpoints, including quality assurance testing, staged deployment, and management review.

5.4.3. **Internal Testing**. Internally, ComplianceWare undergoes periodic risk assessments, including technical vulnerability discovery and analysis of business risks and concerns, source code review, architecture review, code commit peer review, and threat modeling.

6. Contingency Planning.

6.1. High Availability and Failover. Every ComplianceWare Cluster is deployed as a self-healing dyno-set that provides automatic failover in the event of a failure. Similarly, ComplianceWare Nodes will fail across multiple availability zones within a region, providing resilience to localised site failures.

6.2. Backups. ComplianceWare backups are Cloud Provider snapshots, which use the native snapshot functionality of the selected Cloud Provider to locally back up your Customer Data. Cloud Provider snapshots are stored with your selected Cloud Provider in the same region as your ComplianceWare Cluster.

6.3. Business Continuity and Disaster Recovery. SWC maintains a business continuity and disaster recovery ("BCDR") plan that includes availability requirements for customer services, including recovery point objectives (RPOs) and recovery time objectives (RTOs) and backup and restoration procedures. In the event of an incident that triggers the BCDR plan, the RPO will depend on your impacted ComplianceWare Cluster and backup configurations.

7. Incident Response and Communications.

7.1. Security Incident Response. In the event that SWC becomes aware of a Data Breach or other security incident, SWC response includes designation of a security incident response team, reporting mechanisms, procedures for assessing, classifying, containing, eradicating, and recovering from security incidents, procedures and timeframes for required notifications to relevant authorities and customers, procedures for forensic investigation and preservation of event and system log data, and a process for post-incident and resolution analysis designed to prevent future similar incidents.

7.2. Security Incident Tracking. SWC maintains an incident tracking system that documents: (i) incident type and suspected cause; (ii) whether there has been unauthorised or unlawful access, disclosure, loss, alteration, or destruction of data; (iii) if so, the categories of data affected by the incident, including categories of personal information; (iv) the time when the incident occurred or is suspected to have occurred; and (v) the remediation actions taken.

7.3. Customer Communications. SWC will notify you without undue delay if we become aware of any Data Breach. Taking into account the information available to us, such notice will include a description of the nature and cause of the Data Breach and the expected resolution time. To the extent possible, we will subsequently update you with information regarding evaluation of the root cause, potential impact, remediation actions taken, and actions planned to prevent a

future similar event.

8. Audit Reporting.

8.1. Third-Party Certifications and Audit Reports. Upon request, and subject to the confidentiality obligations set forth in the Agreement, we will make available to you (or your independent, third-party auditor) information regarding SWC's compliance with the security obligations set forth in these Security Measures in the form of certifications and/or reports.

8.2. Security Questionnaires. No more than once per year, we will complete a written security questionnaire provided by you regarding the controls outlined in these Security Measures.