INFORMATION SECURITY

A briefing on the information security controls at Computershare
INTRODUCTION

Information is critical to all of our clients and is therefore a key focus for Computershare. We host over one hundred and twenty five million records worldwide. The security of these records is of the utmost importance and we continually make sizable investments to protect our information, IT systems, applications, infrastructure and processes.

Computershare has developed a comprehensive global information security framework aligned to ISO/IEC 27002:2013. This framework and its underlying controls are designed to ensure that:

› Computershare information and systems are only available to authorised people with a justified business need;
› Computershare information is not disclosed or modified without authorisation;
› Computershare information is available when required by relevant business processes;
› applicable regulatory, legislative and client requirements are met;
› information security training is available to all employees;
› breaches of security and suspected weaknesses are reported, investigated, documented and resolved;
› employees have access to relevant additional standards and guidelines that support this policy; and
› our brand and financial resources are otherwise protected from the damage that information security breaches can cause.

This document provides an overview of our information security framework that is in place across all of our businesses.
1. Information Security Policy
Computershare has an Information Security Policy Framework (ISPF) that is aligned to ISO/IEC 27002:2013 and applies to all Computershare business units in all geographic locations. It is owned by the Chief Information Security & Risk Officer, reviewed by key stakeholders across the organisation and approved by the Chief Executive Officer.

The ISPF is the collective term for our Information Security Policy, Information Security Standard, Technical Security Standards and Information Security Guidelines. It is reviewed on an annual basis to reflect any significant changes in Computershare’s structure, business functions and the regulatory environment; or in response to new and emerging information security threats.

The ISPF is communicated to all employees through an information security awareness and training programme and is published via the Information Security Portal on the Computershare intranet.

2. Organisation of Information Security
Computershare has established an effective, forward-looking information security operating model that is supported by a strong professional capability across the organisation.

The Chief Information Security & Risk Officer leads the Global Information Security and Risk Group, providing oversight and guidance on the overall development and implementation of information security across the business. This team works in conjunction with Computershare’s business units and other support functions including Compliance, Audit, and Technology.

All Computershare employees (including consultants, contractors, business partners and suppliers) have their information security responsibilities clearly defined in the Information Security Policy. Specific responsibilities are also included for Line Managers, Information Owners, Information Custodians and Business Unit Heads.

Computershare operates global vendor management programmes to identify, assess and manage the information security requirements that are contractually agreed with our third party suppliers that may access, store, process or transmit information on our behalf.

3. Asset Management
Computershare has implemented an information classification scheme for all information that supports its day to day business activities. Computershare maintains inventories of its information assets, including applications and IT systems. Information Owners and Information Custodians are assigned to all business applications and are required to complete an information security risk assessment. This classifies the application based upon business criticality and identifies the required controls to protect the confidentiality, integrity and availability of the application throughout its lifecycle in accordance with the classification.

At the end of the information lifecycle, all information is securely destroyed prior to reuse or disposal of the information asset.

4. Human Resource Security
All Computershare employees are subject to screening prior to employment. The screening processes are conducted in accordance with relevant national laws and industry regulations and provide verification of identity and credentials, as well as evaluating applicant integrity.

All Computershare employees are subject to confidentiality/non-disclosure agreements as part of the standard employment contracts and are required to comply with the controls outlined in the Information Security Policy, including Acceptable Use of Computershare Information. The Global Information Security and Risk Group manage multi-lingual information security awareness and training programmes to ensure that all employees are aware of their responsibilities and possess the necessary resources to maintain our position on information security. These programmes include mandatory annual on-line training for all employees, targeted security campaigns that are commensurate with specific job roles and more detailed technical security training for the Computershare technology teams.

When an employee leaves, Computershare applies robust procedures to ensure the timely removal of access rights to Computershare’s IT systems as well as the retrieval of physical information assets which are recorded in the asset inventories.

5. Physical and Environmental Security
All Computershare office locations operate risk-based controls to afford protection against unauthorised physical access. These can include physical and electronic access control systems, manned reception desks, CCTV and security lighting. Access to our data centre facilities and other critical information processing locations is strictly controlled.
and restricted to pre-authorised individuals only. This access is logged and the access rights are reviewed on a regular basis.

All Computershare data centre facilities are designed to be protected against fire, flood, environmental and other natural hazards. Our environmental controls can include fire detection and prevention, dual power supplies, monitored Uninterruptable Power Supply (UPS), back-up generators, temperature, smoke, water and humidity controls.

6. Communications and Operations Security

Computershare has implemented a defence-in-depth approach to protect its information and IT systems from existing and emerging threats. The management and operation of our IT systems is delivered by our highly experienced Technology teams using a service management model based upon the Information Technology Infrastructure Library (ITIL) standard. This includes the formalisation of processes and procedures to support core activities such as back-up and recovery, change management, release management and capacity planning.

Computershare has a common resilient split-site and disaster tolerant network and computing architecture design across all of its global data centres. Our multi-tier internet-facing infrastructure uses two physical layers of firewalls supporting three-tier application deployment and secure segregation of different networks, connections and systems where appropriate. Server virtualisation provides rapid resource provisioning and enhanced failover and disaster recovery capabilities.

All Computershare IT systems are configured following documented technical security standards which include applicable controls such as system hardening, encryption, antivirus and malware protection and a regular patching schedule that is defined by the system's criticality and threat level. The Global Information Security and Risk Group actively monitors the internal and external threat environment and works with the Technology teams to ensure that the current security controls deployed are both appropriate and effective, to mitigate risk.

The Computershare IT network is monitored by a global 24x7 Security Operations Centre which collects and correlates the event logs from network devices, firewalls, IDS and web application firewalls. This data is analysed and any unusual or suspicious events generate the necessary alerts which are handled by our information security incident management processes.

7. Access Control

Computershare operates on the principle of ‘least privilege’ for access control. This is to ensure that only authorised individuals are permitted access to our business applications, systems, networks and computing devices, that individual accountability is established and to provide authorised users with the access permissions that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

Our authentication and authorisation mechanisms and processes are commensurate with the criticality of the Computershare IT system. Access is co-ordinated through the regional IT Service Desks and all access requests must be authorised by an employee’s line manager and/or the assigned resource owner. The Global Information Security and Risk Group regularly performs recertification reviews of user access rights to detect and remove any inactive accounts and inappropriate access permissions.

All Computershare employees are assigned unique user IDs and are required to select and manage their passwords in line with the Acceptable Use section of the Information Security Standard. In the event of a change of employment status or role, user access rights are immediately revoked or reassigned by the regional IT Service Desks upon notification from the line manager.

The use of privileged accounts is strictly controlled and restricted to system administration and maintenance activities only. Additional measures are employed to securely manage these accounts. This includes enhanced password management controls and more frequent recertification reviews.

Remote access to the Computershare network is only permitted for pre-authorised employees using a Computershare managed asset. This is achieved using an encrypted VPN solution that performs security validation checks against the asset and is supported by multi-factor authentication.

8. Information System Development, Acquisition & Maintenance

Computershare has a wealth of in-house experience in delivering best-in-class business applications and IT systems. We follow a defined System Development Life Cycle (SDLC) that incorporates information security throughout each stage including risk assessments, the identification and implementation of control requirements, static and dynamic code analysis and technical security penetration testing.

Computershare maintains separate development, test and production environments and has strict policies to enforce segregation of duties for employees responsible for development, testing and support activities. Our source code, including
all applications under development, are stored and protected in an approved source code system with audit logging enabled to track activity such as code modification and deletion.

Our business applications and IT systems classified as critical by the information security risk assessment process have enhanced information security controls and are registered under a ‘permanent supervision programme’ for regular security assurance tests in the production environment.


Computershare has an established global Business Continuity Management programme that supports our regulatory and contractual requirements. Our programme is managed by dedicated regional business continuity resources and is underpinned by relevant business continuity policies, procedures and supporting technologies.

All Computershare business units are included within the Business Continuity Management programme and are required to complete a risk assessment and business impact analysis. This provides a consistent methodology to define the recovery time objectives which are incorporated into specific business continuity plans.

Our business continuity plans and disaster recovery plans are developed and maintained by assigned owners from the Business Units and Technology teams and are regularly updated to reflect any change of circumstances.

Computershare performs business continuity and disaster recovery tests on a periodic basis to ensure that the plans can be employed should the need arise.

The test results are communicated to our senior executive management and relevant stakeholders upon completion.

10. Information Security Incident Management

Computershare has global risk-based processes to respond to information security incidents, unusual or suspicious events and breaches of policies. These processes are owned and co-ordinated by the Global Information Security and Risk Group with formal involvement from relevant stakeholders (e.g. legal, compliance, technology, human resources, business relations and anti-fraud and public relations).

The information security incident management processes are designed to contain and control the incident, reduce any potential impact to the business, identify and investigate the root cause and implement corrective actions to reduce the risk of recurrence. These processes are supported by procedures for identification, reporting, assessment, response, recovery and follow-up. Our post-incident procedures include root cause analysis, forensic investigation and, where required, notification to the relevant authorities and affected clients.

All Computershare employees are provided with training and guidance to identify and report information security incidents. The individuals responsible for managing information security incidents are supported by more specific training and access to relevant tools to complete each stage of the information security incident management process.

11. Compliance

Computershare has an established governance, risk and compliance model that is endorsed by our Risk and Audit Committee. Global Information Security and Risk Group measures compliance with the Information Security Policy through periodic technical and non-technical control assessments. Our technical control assessments include system patch verification, application and infrastructure vulnerability scans and penetration tests.

Computershare has an independent Internal Audit function that delivers global and regional IT and integrated audit reviews which includes the assessment of our processes and technologies against the Information Security Policy. The results of these reviews are documented, managed through to remediation and reported to the Risk and Audit Committee on a regular basis.

Computershare also commissions a number of external audits to provide an independent assurance and attestation of our business and technology controls. These external audits include AT101, ISAE3402 and SSAE16 and are applicable to specific Business Units and geographic locations.

SUMMARY

We trust this demonstrates the commitment and considerable investment Computershare has made to information security and that our clients, business partners, employees and shareholders can have full confidence in the confidentiality, integrity and availability of our information and IT systems.

If you have any specific questions or would like additional information on the measures that we take to protect your information, then please contact your nominated Computershare Relationship Manager.
Computershare (ASX:CPU) is a global market leader in transfer agency and share registration, employee equity plans, proxy solicitation and stakeholder communications. We also specialise in corporate trust, mortgage, bankruptcy, class action, utility and tax voucher administration, and a range of other diversified financial and governance services.

Founded in 1978, Computershare is renowned for its expertise in high integrity data management, high volume transaction processing and reconciliations, payments and stakeholder engagement. Many of the world's leading organisations use us to streamline and maximise the value of relationships with their investors, employees, creditors and customers.

Computershare is represented in all major financial markets and has over 16,000 employees worldwide.

For more information, visit www.computershare.com