CYBERSECURITY MANUAL

V2.0 Issued 05.2024

CONTENTS

1 POLICY

1.1 Policy statement

This Company is committed to ensuring, so far as is reasonably practicable, the protection and security of Company and client data stored on electronic data processing and storage systems owned and used by the Company (including remote storages) and of our technology infrastructure.

1.2 Aims and Objectives

The Company recognises the importance of protecting systems and data from unauthorised access and corruption. To achieve this, we will develop and implement security measures and processes to prevent loss or damage to systems and data from cybersecurity threats, social engineering fraud risks, malicious software and unauthorised use of artificial intelligence (AI).

We will inform and train workers, employees and other persons (including customers and clients) on risks of cybersecurity threats and control measures to be followed and reporting systems and procedures to be followed where a threat to cybersecurity is suspected.

1.3 Responsibilities

Management of the company will be responsible for the development and implementation of a plan for mitigating the effect of social engineering attacks, and for raising awareness and educating employees of cyber-security risks.

Employees using personal or company-issued computers and devices will be instructed in cybersecurity measures to protect confidential data from security breaches and social engineering fraud risks.

Employees are responsible for ensuring that their on-line activities (including the use of AI) do not expose the company to risks of cyber-security and social engineering attacks by adhering to company policies and rules regarding use of company computer systems, use of computers and devices to access company computer systems, and to report perceived

attacks, suspicious emails or phishing attempts as soon as possible to company IT personnel.

2 PURPOSE

The purpose of this document is to ensure that the Company has adequate controls and review procedures to restrict access to computer systems and confidential information and data.

The cybersecurity policy and procedures provides guidelines and processes for preserving the security of Company technology infrastructure and the confidential data of the Company and its clients and customers from cyberattacks and social engineering fraud.

3 SCOPE

The Cybersecurity Policy and Procedures apply to all IT systems or applications managed by the Company that store, process or transmit information, all communications systems and applications, and apply to all employees, consultants, contractors and authorised users accessing Company IT systems and applications.

4 RISK MITIGATION STRATEGIES

The Australian Cyber Security Centre (ACSC) has developed mitigation strategies (the Strategies to Mitigate Cyber Security Incidents) to assist organisations to mitigate cybersecurity incidents caused by various cyber threats. These have been prioritised in a suggested implementation order to assist organisations to build a strong cybersecurity defence for their systems.

The ACSC has also identified maturity levels based on the level of implementation of each mitigation strategy:

- Maturity Level One: partly aligned with the intent of the mitigation strategy
- Maturity Level Two: mostly aligned with the intent of the mitigation strategy
- Maturity Level Three: fully aligned with the intent of the mitigation strategy.

Once organisations have implemented their desired mitigation strategies to an initial level, they should focus on increasing the maturity of their implementation until they eventually

reach full alignment (or a level that is appropriate and satisfactory for the organisation) for each mitigation strategy.

The ACSC recommends that as a baseline, organisations should aim to reach Maturity Level Three for each mitigation strategy. Maturity levels for each mitigation strategy are listed in Appendix 1 of this manual.

4.1 Mitigation strategies to prevent execution of malware

4.1.1 Application control

The application control strategy prevents all non-approved applications (including malicious code) from executing. Organisations should implement application control to prevent execution of unapproved and/or malicious applications including executables and installers (e.g., .EXE, .MSI), dynamic link libraries (e.g., .DLL), scripts (such as .BAT batch files, Windows Script Host, PowerShell and HTA).

4.1.2 Configure macro settings

Macros can be used by attackers to deliver and execute malicious codes on systems. Configure macro settings in applications (such as Microsoft Office) to block macros from the internet, and only allow vetted macros either in trusted locations with limited write access or digitally signed macros with a trusted certificate.

4.2 Mitigation strategies to limit the extent of cybersecurity incidents

4.2.1 Restrict administrative privileges

Administration accounts allow adversaries to gain full access to information and systems.

Restrict administrative privileges to operating systems and applications based on user duties, and regularly revalidate the need for privileges. For example, privileged accounts should not be used for reading email or web browsing.

4.2.2 Multi-factor authentication

Stronger user authentication makes it harder for adversaries to access sensitive information and systems.

Implement multi-factor authentication including for virtual private networks (VPNs), remote desktop protocol (RDP), secure shell (SSH) and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high availability) data repository. (See also ***6.4.2 User authentication***).

4.3 Mitigation strategies to recover data and system availability

4.3.1 Daily backups

Daily backups ensure that information can be accessed following a cybersecurity incident (e.g., ransomware incident).

Implement daily backups of important new or changed data, software and configuration settings, and store disconnected and retain for at least three months. Test restoration initially, annually and when IT infrastructure changes.

4.3.2 Patch applications

Patch applications to prevent risk to security vulnerabilities from applications being used to execute malicious code on systems.

Patch applications with known vulnerabilities (e.g., Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch or mitigate computers with extreme risk vulnerabilities within 48 hours and use the latest version of applications.

4.3.3 Use application hardening

Applications such as Flash, ads and Java are popular ways to deliver and execute malicious code on systems. Configure web browsers to block Flash (or ideally uninstall it), ads and Java on the internet. Disable unneeded features in applications (e.g., OLE in MS Office), web browsers and PDF viewers.

4.3.4 Patch operating systems

Security vulnerabilities in operating systems can be used to assist in enabling the compromise of systems.

Patch or mitigate computers (including network devices) with extreme risk vulnerabilities within 48 hours.

Use the latest operating system version, and do not use unsupported versions.

5 NETWORK AND EQUIPMENT SECURITY

5.1 Scope

These network and equipment security controls apply to:

- employees, consultants, contractors and authorised users accessing company information technology (IT) systems and applications (whether on the premises of the company or related entities, or at a remote location within Australia or overseas)
- IT hardware systems (including servers, workstations, and infrastructure
- data storage and processing equipment
- communications technology (including internet, social media and mobile phones), and
- the use of IT equipment and communications technology, and access to data and prohibited system and network activities.

5.2 General use of networks and equipment

Users may access or use company networks and equipment only to the extent to which it is authorised and necessary to fulfill assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use of company systems and assets (where this is allowed or permitted by the company). Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

For security and network maintenance purposes, authorised individuals within the company may monitor equipment, systems and network traffic at any time.

The company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

5.3 Security of systems and proprietary information

5.3.1 Protection against malicious code

Protection against malicious codes requires the use of antivirus protection and firewall protection on endpoint devices (e.g., desktop/workstations, laptops, and mobile devices). Additionally, all computers running a Windows operating system that hold company data must have automated Microsoft security updates enabled.

Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that process company or customer information must be encrypted using approved software.

Antivirus software must be scheduled to perform daily threat-definition updates and virus scans.

Company IT staff will ensure that antivirus products and Windows Server Update Services (WSUS) are maintained and up to date with virus definitions and security updates. IT is responsible for notifying internal company system users of both any credible virus threats and when security updates are available.

Employees are prohibited from altering, disabling or removing antivirus software and the security update service from any computer. Any employee violating this direction may be subject to disciplinary action up to and including termination of employment.

5.3.2 Network controls

The company will implement and maintain strong network controls for the protection and control of customer data during its transmission from one end system to another. Computers, servers, and other data devices connected to the company network must comply with well-established standards for security, configuration and access methods.

Access to the company network by members and third parties is subject to limitations and prior approval in accordance with company third-party network access protocols.

5.3.3 Protection against unauthorised access

All use of mobile and computing devices that connect to the company network must comply with the principles set out in ***User Access Management*** in this document.

System level and user level passwords must comply with the Password Policy and Principles. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Users must lock the screen or log off when the device is unattended.

Employees must use extreme caution when opening e-mail attachments received from unknown senders and which may contain malware.

5.4 Unacceptable use of company systems and equipment

The company should identify and prohibit activities which may place the security of company systems, networks and equipment at risk of damage or corruption. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the company authorised to engage in any activity that is illegal under local, state, federal or international law while utilising company owned resources.

5.4.1 System and network activities

Unacceptable system and network activities are listed in Appendix 2 of this manual. The list is by no means exhaustive but attempts to provide a framework for activities which fall into the category of unacceptable use.

Any employee found to have violated company rules for unacceptable use may be subject to disciplinary action up to and including termination of employment for serious and deliberate breaches. Other users (consultants, contractors, clients and customers, etc., may have access rights and privileges suspended, rescinded or revoked at the company's discretion.

5.4.2 Information technology and equipment

To ensure the security of the company's IT environment, employees and users may not under any circumstances except with the written approval of a departmental manager and the IT Manager:

- load or run any third-party software which the company is not licensed to use on any company computer or device.
- remove any company hardware or software (including but not limited to third-party software which the company is licensed to use from any company location).

Any equipment provided by the company is for the sole purpose of work for the company, and personal use of this equipment without prior authorisation is strictly prohibited. (Note: legislative amendments have ruled personal use of company equipment liable for Fringe Benefits Tax (FBT)).

6 INFORMATION SECURITY

6.1 Scope

These information security controls apply to:

- employees, consultants, contractors and authorised users accessing company information (IT) systems and applications (whether on the premises of the company or related entities, or at a remote location within Australia or overseas)
- data storage and processing equipment
- software and applications (proprietary or bespoke)
- communications technology (including internet, social media and mobile phones), and

- the use of IT equipment and communications technology, and access to data and prohibited system and network activities.

The management of information security will be aligned with the international standard ISO IEC 27001:2023 *Information security, cybersecurity and privacy protection – Information security management systems – Requirements* and requirements of regulations and other relevant standards.

6.2 Definitions

Confidential Information means any information in respect of the business and affairs of this company, its clients and suppliers that is not in the public domain including, without limitation, any document, record, computer file, customer information, product or service information, sales or financial information, discovery, invention, drawing, design, strategy, plan, data, report, process, proposal, budget, idea, concept or know how.

Employee means any individual employed by this company.

Social Media means any platform for online publication and commentary, including without limitation:

- social and professional networking sites (e.g., Facebook, LinkedIn).
- video, audio and photo sharing websites (e.g., Flickr, YouTube).
- blogging and micro-blogging sites (e.g., Twitter, WordPress).
- discussion boards and forums (e.g., Google Groups).and
- online encyclopaedias (e.g., Wikipedia).

6.3 Ownership and general use of information

Proprietary information stored on electronic and computing devices whether owned or leased by the company, an employee or a third party, remains the sole property of the company. Users must ensure through legal or technical means that proprietary information is protected in accordance with the controls set out in this document.

Employees and users have a responsibility to promptly report the theft, loss or unauthorised disclosure of any company proprietary information.

Users may access, use or share proprietary information only to the extent it is authorised and necessary to fulfill assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use of company systems and assets. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

Postings by employees from a company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Company, unless posting is in the course of business duties.

For security and network maintenance purposes, authorised individuals within the company may monitor equipment, systems and network traffic at any time.

The company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

6.4 Security of systems and proprietary information

6.4.1 Protection against malicious code

Protection against malicious codes requires the use of antivirus protection and firewall protection on endpoint devices (e.g., desktop/workstations, laptops, and mobile devices). Additionally, all computers running a Windows operating system that hold company data must have automated Microsoft security updates enabled.

Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that process company or customer information must be encrypted using approved software.

Antivirus software must be scheduled to perform daily threat-definition updates and virus scans.

Company IT staff will ensure that antivirus products and Windows Server Update Services (WSUS) are maintained and up to date with virus definitions and security updates. IT is

responsible for notifying internal company system users of both any credible virus threats and when security updates are available.

Employees are prohibited from altering, disabling or removing antivirus software and the security update service from any computer. Any employee violating this direction may be subject to disciplinary action up to and including termination of employment.

6.5 Artificial Intelligence

Artificial intelligence (AI) has emerged as required technology for augmenting the efforts of human information security teams. AI can identify and prioritise risk, instantly spot any malware on a network, guide incident response, and detect intrusions before they start. AI improves staff efficiency and reduces the risk of human error and manages significantly more data than a human security team could.

6.4.1 Application of artificial intelligence

AI can assist in detecting and preventing cyber threats by analysing network traffic, identifying anomalies, and predicting potential attacks. It can enhance the security of systems and data through advanced threat detection and response mechanisms.

However, AI can also pose a risk to cybersecurity and the risks of artificial intelligence to cyber security are expected to increase rapidly with AI tools becoming cheaper and more accessible.

6.4.2 *Roles of AI in cyber security*

Risks from AI to cyber security include:

- *Cyber attack optimisation* –generative AI and large language models are used to scale attacks to optimise phishing attack techniques.
- *Automated malware* –AI is used to create malicious codes and bypass existing protections.
- *Physical safety* –risks to physical safety of persons and property from cyber security breaches to systems such as autonomous vehicles, manufacturing and construction equipment and medical systems, etc.

- *Privacy risks* –AI systems designed for marketing, advertising, profiling, or surveillance are used to access sensitive information and invade user privacy.
- *Data manipulation and poisoning* – occurs when an attacker modifies or poisons training data with malicious data to produce unexpected or even malicious outcomes.
- *Reputational damage* – an organisation that uses AI can suffer reputational damage if the technology malfunctions or it suffers a cyber security breach which results in data loss and the organisation facing fines, civil penalties and deteriorating customer relationships.

Protections from risks from AI include:

- *Auditing of any AI systems in use* – Check the current reputation of any AI system in use to avoid security and privacy issues and audit systems periodically to detect and address vulnerabilities to reduce AI risks.
- *Limiting sharing of personal information through automation* – Avoid sharing of personal information with AI.
- *Data security* - AI relies on its training data to deliver good outcomes and can deliver unexpected and dangerous results if the data is modified or poisoned. Protect AI from data poisoning by use of cutting-edge encryption, access control, and backup technology. Secure networks with firewalls, intrusion detection systems, and sophisticated passwords.
- *Optimised software* - Follow all best practices of software maintenance to protect from the risk of AI. This includes updating AI software and frameworks, operating systems and apps with the latest patches and updates to reduce the risk of exploitation and malware attacks. Protect systems with next-generation antivirus technology to stop advanced malicious threats and invest in network and application security measures to harden defences.
- *Adversarial training* - Adversarial training is an AI-specific security measure that helps AI respond to attacks. The machine learning method improves the resilience of AI models by exposing them to different scenarios, data, and techniques.
- *Vulnerability management* – AI vulnerability management can mitigate the risk of data breaches and leaks. Vulnerability management is an end-to-end process that involves identifying, analysing, and triaging vulnerabilities and reducing attack surfaces related to the unique characteristics of AI systems.

6.4.3 Training and response

Training of personnel who may impact network and information security is essential to ensuring protection from and response to cyberthreats and attacks. Regular updating of

systems and refresher training is essential in maintaining awareness and effective response to any threat to or attack on the cybersecurity of an organisation.

- *Staff training* – train employees in AI risk management to counter threats of phishing attacks from AI generated emails and unsolicited software containing malware created by artificial intelligence.
- *AI incident response* – Organisations may suffer an AI-related cyber security attack despite having the best security measures as the risks of artificial intelligence grow. All organisations should have a clearly outlined incident response plan that covers containment, investigation, and remediation to recover from such an event.

7 USER ACCESS MANAGEMENT

7.1 Scope

User Access Management controls apply to:

- all offices and data centres of the company.
- all employees, consultants, and authorised users accessing company IT systems and applications either directly or via remote access.
- all IT systems or applications managed by the company that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

Ensuring that the requirements for access to systems and their resources are documented and agreed upon helps determine if personnel have the appropriate authorisations, security clearances and need-to-know to access a system and its resources.

Types of users for which access requirements should be documented include standard users, unprivileged and privileged users, vendors and contractors, and external users (e.g., clients, customers, etc.).

7.2 Account types

7.2.1 Administrative accounts

Regular User Account	Unprivileged Administration Account	Privileged Administration Account
Unprivileged account	Unprivileged account	Privileged account
Used for web and email access Used for day-to-day non-administrative tasks	Used for authentication to dedicated administrator workstation Used for authentication to jump server(s)	Used for performance of administration tasks
	Different username and passphrase to regular user account	Different username and passphrase to regular user account

7.2.2 Security of administrative accounts

The use of the same credentials on both an administrator workstation and a user workstation will put the administrator workstation at risk of compromise if the user workstation is compromised.

One of the greatest threats to the security of a network as a whole is the compromise of a workstation used for administration activities. Providing a physically separate hardened administrator workstation to privileged users, in addition to their workstation used for unprivileged user access, provides greater assurance that privileged activities and credentials will not be compromised.

Using different physical machines is considered the most secure solution to separate workstations; however, a risk-based approach may determine that a virtualisation-based solution is sufficient. In such cases, the unprivileged user environment should be the ‘guest’ and the administrative environment should be the ‘host’.

Administration security can be improved by segregating administrator workstations from the wider network. This can be achieved a number of ways, such as via the use of Virtual Local Area Networks (VLAN), firewalls, network access controls and internet protocol security server and domain isolation.

It is recommended that segmentation and segregation be applied regardless of whether privileged users have physically separate administrator workstations or not.

7.3 General access security requirements

The company will provide access privileges to information technology (including networks, systems, applications, computers and mobile devices) based on the following principles:

- need to know - employees will be granted access to systems that are necessary to fulfill their roles and responsibilities.
- least privilege - employees will be provided with the minimum privileges necessary to fulfill their roles and responsibilities.

Requests for accounts and access privileges must be formally documented and appropriately approved.

Requests for special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, shared/generic accounts, test accounts and remote access) must be formally documented and approved by the IT Manager.

Application and service accounts must only be used by application components requiring authentication; access to the passwords must be restricted to authorised IT administrators or application developers only.

Where possible, the company will set user accounts to automatically expire at a pre-set date. More specifically,

- when temporary access is required, such access will be removed immediately after the employee has completed the task for which the access was granted.
- accounts assigned to contractors/clients will be set to expire according to the contract's expiry date.
- accounts will be disabled after 3 months of inactivity.

Access rights will be immediately disabled or removed when an employee is terminated or a user ceases to have a legitimate reason to access the system.

Verification of an employee or user's identity must be performed before granting access to the system. Issue of passwords should be automated where applicable.

Existing accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privileges include:

- an active account assigned to external contractors, vendors, clients or employees that no longer work for or use the services of the Company.
- an active account with access rights for which the employee's role and responsibilities do not require access.
- system administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to an employee who is no longer an administrator.
- unknown active accounts.

All access requests for system and application accounts and permissions will be documented using the ticketing system in place.

7.4 User access controls

Authorisation of access privileges for users is dependent upon the identified requirements of the tasks assigned to or to be carried out. Authorisation decisions for granting higher levels of access must be made and reviewed by company management in consultation with the IT Manager.

Granting, approval and review of access will be made based on the following principles:

- need to know: Does the user require this access for their job function?
- segregation of duties: Will the access result in a conflict of interest?
- least privilege: Is access restricted to only those resources and information required for a legitimate business purpose?

7.4.1 Privileged accounts

A nominative and individual privileged user account must be created for administrator accounts, instead of generic administrator account names.

Privileged user accounts can only be requested by managers or executives and must be appropriately approved.

7.4.2 Shared user accounts

Shared user accounts are only to be used on an exception basis with the appropriate approval. This includes general user accounts such as ‘guest’ and ‘functional’ accounts.

When shared accounts are required:

- passwords will be stored and handled in accordance with the User Authentication Policy.
- the use of shared accounts will be monitored where possible, including the recording of the time of access, the reason for accessing the shared user account, and the individual accessing his account.

When the shared user account has administrative privileges, such a procedure is mandatory and access to the monitoring logs must be protected and restricted.

7.4.3 Vendor and default accounts

Where possible, all default user accounts will be disabled or changed. These accounts include ‘guest’, ‘temp’, ‘admin’, ‘administrator’, and any other commonly known or used default accounts, as well as related default passwords used by vendors on “commercial off-the-shelf” systems and applications.

7.4.4 Test accounts

Test accounts can only be created if they are justified by the relevant business area or project team and approved by the application owner through a formal request to the IT Manager.

Test accounts must have an expiry date (maximum of 90 days). Maintaining test accounts beyond this date must be re-evaluated every 90 days and approved appropriately.

Test accounts will be disabled or deleted when they are no longer necessary.

7.4.5 Contractors and vendors

Contracts with contractors or vendors will include specific requirements for the protection of data. In addition, contractor and vendor representatives will be required to sign a Non-

disclosure Agreement (NDA) prior to obtaining approval to access the company's systems and applications.

Prior to granting access rights to a contractor or vendor, the IT Manager must verify the requirements listed in the preceding paragraph have been complied with.

The company will maintain a current list of external contractors or vendors having access to the company systems and reviewed.

7.5 Access security controls

Protection of access to company systems is critical to maintaining the integrity of systems and to prevention of unauthorised access to company information and data of clients and customers. Access to systems and sensitive and/or confidential data will be controlled in accordance with the company's User Authentication Policy.

User access is controlled through an account management system that is integrated with the company's human resources database. Access privileges are granted based on job roles and requirements and require management approval.

7.5.1 User authentication controls

All employees and authorised users who require access to company systems and applications must have a unique login. Passwords must be set in accordance with the company's Password Policy.

Employees must follow rules for password length and complexity and keep their passwords confidential and secured at all times. Passwords may not be disclosed to unauthorized persons. Under certain circumstances, company employees may share passwords with authorised persons providing support services.

Remote access to systems and applications should use two-factor authentication where possible.

System and application sessions should automatically lock after 10 minutes (or other time specified by management) of inactivity.

7.5.2 User authentication

It is essential that users are authenticated before being granted access to a system or its resources. This is typically achieved by single-factor authentication (e.g., username and password or passphrase) or multi-factor authentication (e.g., username together with biometrics and a password or passphrase).

Multi-factor authentication uses two or more authentication factors to confirm a user's identity including:

- something a user knows, such as a password or passphrase
- something a user has, such as a universal 2nd factor security key, physical one-time password token or smartcard
- something inherent to a user, such as a fingerprint or their facial geometry.

(Note: if something a user knows is written down, or typed into a file and stored as plaintext, this becomes something that a user has rather than something a user knows).

It is important that multi-factor authentication is used for accounts which are more likely to be targeted by an attacker such as privileged users, administrators, and users with access to important data repositories.

Multi-factor authentication may be implemented as part of a jump server authentication process rather than performing multi-factor authentication on all critical assets, some of which may not support multi-factor authentication.

7.6 Compliance monitoring

The IT Manager will verify compliance with these user access controls through various methods, including but not limited to, periodic walk throughs, video monitoring, business tool reports, internal and external audits, and feedback to company management.

7.6.1 Exceptions

Any exceptions to the user access controls must be approved by the IT Manager in advance of the exception.

7.6.2 Non-compliance

An employee found to have violated user access and authentication controls may be subject to disciplinary action, up to and including termination of employment. Other users may have access rights rescinded and other action taken at the discretion of company management.

8 APPLICATION SECURITY

This section covers all web application security assessments for the purposes of maintaining the security posture, compliance, risk management, and change control of company technologies.

8.1 Application security assessments

All web application security assessments will be performed by personnel either employed or contracted by the company. All findings are considered confidential and are to be distributed to persons on a “need to know” basis. Distribution of any findings outside of the company is strictly prohibited unless approved by the IT Manager.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

Web application security assessments must be carried out on all applications and subsequent releases unless exempted. Any web applications that do not comply with security requirements may be taken offline until such time that a formal assessment can be performed at the discretion of the IT Manager.

8.2 Security assessment criteria

Web applications will be subject to security assessments based on the following criteria:

- new products will undergo a full security assessment prior to release into the live environment.
- major releases or large new features that involve large changes to the existing product will undergo a full security assessment or targeted security assessment prior to release into the live environment.

- small releases that include feature changes or improvements and small new features will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
- emergency release features will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
- full security assessments will be conducted periodically on all applications in the live environment.

8.2.1 Determination of application security issues

All security issues that are detected during assessments must be mitigated based on their security risk levels. Testing must be carried out to validate fix and/or mitigation strategies for any discovered issues of medium risk level or greater:

- High/Critical: Any high risk or critical risk issue must be fixed immediately, or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.
- Medium: Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
- Low: Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

8.2.2 Security assessment levels

Assessment of security risks should be carried out according to the following assessment levels:

- **Full**: A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
- **Quick**: A quick assessment will consist of an automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

- **Targeted**: A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

8.3 Application fixes

Details and maturity levels for application security and mitigation strategies are listed in Appendix 1 of this manual.

9 DATA PROTECTION

9.1 Preservation of digital data

9.1.1 Digital continuity planning

The company will plan for and implement processes and procedures for digital continuity to assist in ensuring the long-term integrity and availability of important data and information and by taking into account the potential for data degradation and obsolescence of media, hardware and software.

9.1.2 Data backup and restoration

The company will implement data backup and restoration processes and procedures as an integral part of company business continuity and disaster planning and digital preservation strategy.

Backup of all important information (software, and configuration settings for software, network devices, and other ICT equipment) should be carried out on a daily basis to ensure that important information will not be lost and business operations will have a reduced downtime in the event of a ransomware attack on the system.

9.2 Backup storage and retention

9.2.1 Backup storage

Backups must be protected from unauthorised modification, corruption and deletion to mitigate the likelihood of information becoming unavailable due to accidental or malicious deletion of backups.

Backups should be stored offline, preferably at multiple geographically dispersed locations, or online in a non-rewritable and non-erasable manner (e.g., use of 'write once read many' technologies).

9.2.2 Backup retention periods

Backups should be stored for at least 3 months or more to allow for the recovery of information.

Organisations are encouraged to consult with relevant retention requirements as set out in the National Archives of Australia's ***Administrative Functions Disposal Authority Express Version 2*** when determining backup retention times.

9.3 Restoration of backups

Full restoration of backups should be tested at least once following the implementation of backup technologies and processes to ensure that backups can be restored when the need arises, and so that any dependencies can be identified and managed.

Full restoration of backups should be tested each time fundamental information technology changes occur (such as when deploying new backup technologies).

It is important that regular testing in the form of partial restoration of backups is undertaken to verify that backups can be restored when necessary.

10 ICT EQUIPMENT AND MEDIA

10.1 ICT equipment and media register

The Company should maintain and regularly audit a register of authorised information and communications technology (ICT) equipment and media to assist in tracking legitimate assets and in determining whether unauthorised assets have been introduced into a system or its operating environment.

10.2 Securing ICT equipment and media

ICT equipment and media should be secured when not in use. This can be achieved by implementing one of the following approaches:

- securing ICT equipment and media in an appropriate security container or secure room.
- using ICT equipment without hard drives and sanitising memory at shut down.
- encrypting hard drives of ICT equipment and sanitising memory at shut down.
- sanitising memory of ICT equipment at shut down and removing and securing any hard drives.

If none of the above approaches are feasible, organisations may wish to minimise the potential impact of not securing ICT equipment when not in use. This can be achieved by preventing sensitive or classified information from being stored on hard drives (e.g., by storing user profiles and documents on network shares), removing temporary user data at logoff, scrubbing virtual memory at shut down, and sanitising memory at shut down.

10.3 Wireless devices and radio frequency transmitters

10.3.1 Radio frequency (RF) devices

Many RF devices (e.g., mobile devices) can pose a security risk when they are capable of picking up and recording or transmitting background conversations. It is important that organisations understand the security risks associated with the introduction of RF devices in highly classified environments and that they should maintain a register of those that have been authorised for use in such environments and ensure that only authorised devices are allowed in those environments.

10.3.2 Bluetooth and wireless keyboards and devices

Controls should be considered for the use of Bluetooth and wireless devices in sensitive environments to prevent unacceptable emanation risks. Use of Bluetooth or wireless devices for communication of sensitive or classified information should be limited to RF screened buildings.

10.3.3 Infrared keyboards

Drawn curtains or screens that block infrared transmission are required as a minimum form of protection in security sensitive areas using infrared keyboards. Depending on the security sensitivity of the area, it may be a requirement that windows are fitted with curtains or screens that cannot be opened to permanently block infrared transmissions.

11 COMMUNICATIONS

11.1 Online services

Email and the Internet have become powerful and widespread communication tools for the exchange of information and knowledge. It is therefore essential that all employees of the company adhere to certain guidelines for the use of these communication tools and employees are to use good judgement at all times.

All personnel using company systems should be provided with cybersecurity training in relation to the use of online services to assist them in understanding their security responsibilities. The content of training will depend on the objectives of the organisation, especially where responsibilities are beyond that of a standard user.

11.1.1 Use of online services

Online services such as email, internet forums, instant messaging apps and direct messaging on social media can all be used by an adversary in an attempt to elicit information from personnel. As such, personnel should be advised of what constitutes suspicious contact via online services and how to report it.

11.1.2 Posting work information to online services

Personnel should be advised to take special care not to post work information to online services unless authorised to do so, especially in internet forums and on social media. (Information that appears to be benign in isolation could, along with other information, have a considerable security impact). Personnel using social media should maintain separate work and personal accounts for online services to ensure that personal opinions of individuals are not interpreted as official policy.

11.1.3 Posting personal information to online services

Any personal information posted to online services (such as social media) could be used by an adversary to develop a detailed profile of a person's lifestyle in order to build a relationship with them. This relationship could then be used to attempt to elicit information or influence the person to undertake specific actions, such as opening malicious emails or visiting malicious websites. Encouraging personnel to use the privacy settings of online services can minimise who can view their information and interactions on such services.

11.1.4 Sending and receiving files

Personnel sending and receiving files via online services such as instant messaging apps and social media may often bypass security controls put in place to detect and quarantine malicious code. Personnel should only send and receive files via authorised online services to ensure that files are appropriately protected and scanned for malicious code.

11.2 Email usage

These guidelines for email usage set out:

- the company's guidelines for acceptable and unacceptable use of email and
- the rights and responsibilities of company users of email on company systems.

In this section, the term 'employee' includes a contractor (or a contractor's employee) given access to the company's email facilities.

11.2.1 Employee use of email

The email system and email transmissions are the property of the company and as such, the company is responsible for the administration and responsible use of the system. Under normal circumstances, an employee's email account is private and strictly confidential. However, if the company considers that inappropriate and/or illegal use of the email account may be occurring, it reserves the right to monitor email accounts and take appropriate action. Users should be aware that all email communications are recorded and deleted emails are recoverable through the email journaling systems that are in place.

The company has the right to grant or remove email access to an employee at its discretion. If, subsequent to an investigation, it can be demonstrated that an employee has breached

the email policy, a formal discipline interview will be conducted. If deemed necessary, the employee will have his or her email access removed. Their ability to function effectively will then be assessed. Subsequent breaches will lead to further disciplinary action and, potentially dismissal.

It is important for all employees and users to realise that there is potential for legal action both against the company and against the individual when they use email. Additionally, it is in the interests of both the company and the employee that personal use of email for non-business-related activity is not excessive. As such, employees are required to adhere to company policies when using email.

11.2.2 Acceptable use of email

Email may be used for the following purposes:

- communications for work-related purposes within the company.
- communications for work-related purposes with people outside the company.
- incidental and occasional personal use of email. Excessive use of email for personal and non-business-related communications is discouraged and it must not interfere with everyday workloads.

11.2.3 Unacceptable use of email

Unacceptable use of email includes:

- excessive distribution of jokes, gossip and rumours.
- email which would be likely to harass, insult or discriminate on the basis of age, sex, race, religion, national origin, sexual orientation, political beliefs, disability or other criteria. Users must be aware that email may render them and/or the company liable for harassment or discrimination claims, and possibly defamation actions.
- junk or chain mail.
- the distribution of information which infringes copyright laws.
- as a means to further personal business activities.
- to further any illegal activity.
- to further any activity in breach of the employee's terms and conditions of employment.
- sending emails so they appear to be from another person.
- distribution of company information to a third party external storage facility (e.g., gmail/hotmail/yahoo or similar)

- distribution of confidential information to third parties without authorisation.

11.3 Internet usage

Use of the Internet by employees should follow the same guidelines as for email usage. In particular, users should be aware that:

- the viewing of pornographic material through the company internet is totally inappropriate and is prohibited.
- material which is defamatory, vilifying or harassing must not be posted, accessed, transmitted or requested via the Internet.
- excessive use of the internet for personal and non-business-related purposes is discouraged and it must not interfere with your everyday workload.
- the internet offers many opportunities to download software to your computer. Under no circumstances should an employee download software without the approval of their manager or the IT department.

The company reserves the right to monitor Internet sites which are accessed by employees and may take appropriate action if it considers that inappropriate and/or illegal use of the internet may be occurring. Personal use of the internet is not permitted during business hours and should only be accessed before and after the employees working hours and during the employee's rest or meal break.

11.4 Mobile devices

11.4.1 Mobile network

All use of mobile devices, including smart phones and tablets, that the company provides to employees and contractors, or used for the company's business purpose, should be solely via the secured company WiFi network where possible. Where a WiFi network is not available or feasible, certain precautions should be taken to defend against mobile security threats.

11.4.2 Mobile device security threats

Mobile devices are vulnerable to a wide range of cyber-attacks that threaten users' privacy, login credentials, finances, and safety. A mobile device security threat exploits vulnerabilities

in mobile software, hardware, and network connections to enable malicious, unauthorised activities on the device. There are many types of mobile security threats, including:

- **Physical**: Stolen or lost mobile devices without adequate security are a high security threat. To mitigate these threats, strong passwords should be used and the device should be set up to lock itself when not in use. Anti-theft tracking software, often built into phone operating systems, should be enabled.
- **Network**: Mobile devices are capable of connecting to multiple networks (including but not limited to WiFi, Cellular, GPS, Bluetooth). Any of these networks can be compromised by attackers to simulate or spoof access to company networks and sensitive data. Users should switch off networks that are not required and change security settings to prevent unauthorised network access.
- **Web-based**: As with computers, mobile devices can often be used to access websites which inherently share the same vulnerabilities including malware and spyware. Security software should be installed on all mobile devices accessing company infrastructure, including networks and email.
- **App-based**: Cyberattacks can occur through malicious mobile apps. These apps, once installed, can potentially steal private data or spend money without the users' permission. To limit these type of threats, mobile device software, including the devices operating system, should be kept up to date to patch invulnerabilities.

11.4.3 Mobile device protection

Mobile device protection measures include:

- Mobile device use should be included in company-wide security policies. These policies should cover acceptable use, anti-theft measures and mandatory security settings.
- If a mobile device is stolen or compromised, an identity and access management (IAM) system should be in place to ensure the malicious user cannot access data on the device or connected networks.
- Security software should be installed on all mobile devices accessing company infrastructure, including networks and email.
- Keep mobile devices locked with secure passcodes or biometrics (fingerprint, or facial recognition) at all times. Mobile devices should auto-lock when not in use.
- Enable data encryption settings where available.

- Remote wipe or reset capabilities are available on most mobile devices and should be enabled, to allow users or the IT department to remotely wipe the device if it is lost or compromised.

11.5 Social media

Persons engaging in the use of social media must be clear about who they are representing and take responsibility for ensuring that any references to the company are factually correct and accurate and do not breach confidentiality requirements. Respect must also be shown for the individuals and communities with whom the company interacts.

Use of social media should follow the rules set out in the company's Social Media Policy; however, this policy does not apply to employees' personal use of social media platforms where the employee makes no reference to the company. Guidelines for the use of social media are listed in Appendix 4 of this Manual.

The following guidelines should be implemented in all use of social media:

- ensure that usage of personal social media is limited to work breaks, and/or before or after standard work hours. The use of social media must not impact on an employee's work in any way
- ensure that any content published is factually accurate and complies with relevant company policies
- employees should not speak about or on behalf of the Company unless authorised by management.

12 SOCIAL ENGINEERING FRAUD RISK

12.1 What is social engineering?

Social engineering is one of the greatest security threats facing business today with hackers continually devising new ways to deceive employees into divulging personal details or sensitive company information. The financial consequences of social engineering fraud can be devastating, and employers must educate employees on how to identify fraud and have the right insurance cover to protect business assets in the event of an attack.

Social engineering is the use of deception to manipulate individuals into voluntarily providing confidential business or personal information that could be used for fraudulent purposes.

Cyber criminals use social engineering tactics to convince victims to click on a malicious link or open email attachments infected with malware, persuade unsuspecting users to hand over sensitive information or even coerce people into installing and running malware.

Social engineering is different from traditional hacking in that the attacks are non-technical and do not necessarily involve the compromise of software or systems, meaning that protections such as firewalls, anti-virus, malware and ransomware software are not a defence. It is the element of human interaction and persuasion that differentiates social engineering from traditional hacking and thus making it more difficult to deal with.

12.2 Types of social engineering fraud

There are a number of strategies used by hackers to gain access to information and systems through people. Some of the more common social engineering tactics include:

- **Phishing** - this most common type of social engineering is typically delivered in the form of phone call or email from someone claiming to be in a position of authority who asks for confidential information, such as a password. Phishing can also include sending emails to organisational contacts that contain malware designed to compromise computer systems or capture personal or private credentials. Attackers may use an email, chat, web ad or website that has been created to impersonate a real organisation (such as a bank, government agency or large corporation). Some phishing messages may ask the user to verify their login details on a mocked-up login page complete with logos and branding to look legitimate. Strategies include requests for bank details to deposit winnings or ask for a donation to a charitable cause (quite often a natural disaster or an emotive tragedy).
- **IVR/Phone phishing (aka vishing)** - this technical tactic involves using an interactive voice response (IVR) system to replicate a legitimate sounding message that appears to come from a bank or other financial institution and directs the recipient to respond in order to “verify” confidential information.
- **Trash cover/forensic recovery** - attackers collect information from discarded materials such as old computer equipment (e.g., hard drives, thumb drives, DVDs, CDs) and company documents that were not disposed of securely.
- **Baiting** - this involves offering something enticing to a user in exchange for login details or sensitive information (baits could be a music or movie download or a corporate branded flash drive). Malware is then placed on the system when the bait is downloaded or used. Another common method of baiting involves leaving an

innocent looking malware-infected device—such as a USB drive, CD or DVD—at a location where an employee will come across it, and then out of curiosity will plug/load the infected device into his or her computer.

- **Quid pro quo (give and take)** - this is similar to baiting and involves the request for login details or sensitive data in exchange for a service (e.g., a hacker posing as a technology expert may call a user and offer free IT assistance or technology improvements to obtain login details).
- **Impersonation/pretexting** – this ruse is the human equivalent of phishing where a hacker poses as an authority figure (often from within the company) to create a false sense of security with the user to gain access to login details.
- **Tailgating / direct access** - also known as piggybacking, tailgating occurs when an unauthorised person physically follows an authorised person into a restricted area or system. The attacker may state that he or she left security credentials inside the facility or at home if challenged by an employee while entering the facility.
- **Diversion theft -** the methodology in this attack involves misdirecting a courier or transport company and arranging for a package or delivery to be taken to another location.

In addition to the methods listed above, attackers using social engineering will focus their attention on locating vital data such as account numbers, phone and client contact lists, organisational charts, and other information on key employees who have access privileges and computer system details (on servers, networks, intranets, etc.) during their information-gathering phase. They have also been known to go after tangible property such as keys, access cards, and identity badges—especially in cases where their method of operation is through direct access.

12.3 Preventing social engineering attacks

The best defence for combating social engineering fraud is awareness through corporate culture, education and training. It is not enough for a workforce to simply follow a policy guideline; employees must be educated on how to recognise and respond to an attacker's methods and thus become a 'human firewall'.

Effective measures to prevent social engineering fraud include:

1. **Education** – this is the best defence against social engineering fraud and requires every employee in the organisation knowing what social engineering is, the common types of fraud, and how to identify and respond to an attack.
2. **Policies and procedures** – employees at all levels must be given a clear set of guidelines on how to respond appropriately to social engineering incidents. Procedures can include setting parameters and verification checks for releasing and exchanging information, requiring at least two-person authorisation to change any vendor or client payment details, reinforcing the importance of building and maintaining security, and warning against accessing unknown security devices.
3. **IT security** – ensure that IT security is kept up to date, including installation of the latest anti-virus software and malware protection, firewalls and email filters.
4. **Insurance** – ensure that business insurance provides cover for losses incurred due to social engineering fraud, including instances where an action was knowingly performed by an employee who has been unknowingly duped by an attacker.

A comprehensive listing of countermeasures to combat social engineering fraud attacks are listed in Appendix 3 of this Manual.

13 DEALING WITH CYBERSECURITY INCIDENTS

Minimising the impact of a cybersecurity incident depends on preparing for an incident before it happens and ensuring that people are aware of how they should respond to the incident. Matters to consider in the development of a cyber security response plan include:

- how to respond to a cybersecurity incident
- what actions to take when an incident occurs, and
- the roles and responsibilities of staff for dealing with a cyberattack.

13.1 Cybersecurity incident response plan

An incident response plan that outlines the steps that need to be followed helps prepare for and respond to a cybersecurity incident. The following stages should be considered when preparing a cybersecurity incident response plan.

13.1.1 Prepare and prevent

The company should:

- prepare the business and employees to be ready to handle cyber incidents.

- develop policies and procedures to help employees understand how to prevent an attack and to identify potential incidents.
- identify the assets that are important to the business – financial, information and technology assets.
- consider the risks to these and the steps that are needed to be taken to reduce the effects of an incident.
- create roles and responsibilities so everyone knows who to report to if an incident occurs, and what to do next.

13.1.2 Check and detect

Check and identify any unusual activities that may damage the business information and systems. Unusual activity may include:

- the company network is not accessible
- user accounts are not accessible
- passwords are no longer working
- data is missing or altered
- hard drives runs out of space
- computers or systems keeps crashing
- customers receive spam from the company business account, and/or
- numerous pop-up ads are being received.

Any person seeing a security incident should document any evidence and report it to either the company IT department, a team member and/or a government body such as the Australian Cybercrime Online Reporting Network.

13.1.3 Identify and assess

The next step is to identify the source and cause of the incident, and to assess the potential impacts on the company. This will require IT staff to:

- find the initial cause of the incident and assess the impact so it can be contained quickly.
- determine the impact the incident has had on business.
- determine its effects on business and assets if not immediately contained.

13.1.4 Respond

Prompt and effective response is essential to:

- limit further damage of the cyber incident by isolating the affected systems. (if necessary, disconnect from the network and turn off computers to stop the threat from spreading).
- eliminate the problem with the removal of the threat.
- recover from the incident by repairing and restoring systems to business as usual.

13.1.5 Review

A review of all incidents should be carried out to:

- identify if any systems and processes need improving and make those changes.
- evaluate the incident before and after, and any lessons learnt.
- update the cybersecurity incident response plan based on the lessons learnt so that the company can improve its business response.

Review and revise the company Cybersecurity Incident Response Plan on a regular basis to include any lessons learnt or critical new information regarding such incidents.

Where changes to the Plan or response to cybersecurity incidents have been made, all staff should be advised of the changes and how they are to respond to any cyber incident in the future.

14 BEST PRACTICES FOR CYBERSECURITY

Data breaches can have severe financial and reputational implications, and businesses can no longer afford to ignore the importance of robust and effective cybersecurity measures. Ensuring that systems are secure is not just about company data but also about maintaining trust and credibility with customers and stakeholders.

Small to medium sized enterprises (SMEs) are particularly prone to cyberattacks due to their often-limited cybersecurity measures. Implementing robust cybersecurity measures should be a company-wide effort and not simply aimed at recognised target areas.

Best practices that can be adopted by businesses to minimise risks of a cyberattack include:

- regular updates of antivirus and anti-spyware on all computers, servers and devices

- installing software updates for operating systems and applications as they become available
- changing manufacturer's default passwords for all software
- use a password manager to create and maintain strong user identification and access control
- using a firewall for internet connections
- regular backups of important data
- controlling physical access to computers, servers and other network components
- secure Wi-Fi networks
- implementing individual user accounts for each employee
- limiting employee access to data and information, and limiting authority for software installation
- monitoring, logging and analysing all successful and attempted attacks on systems and networks, and
- securing mobile phones and devices that contain sensitive information.

Employees play a crucial role in maintaining cybersecurity in an organisation, and should:

- use strong passwords, change then periodically and not share them with anyone
- not use the same password across multiple accounts or services
- protect private information by not disclosing it unless necessary
- not open suspicious links or emails, and ask if unsure
- scan all external devices (such as USB drives) for viruses and malicious software (malware) before using the device.

APPENDIX 1 ACSC MATURITY LEVELS

The Australian Cyber Security Centre (ACSC) has developed mitigation strategies (the Strategies to Mitigate Cyber Security Incidents) to assist organisations to mitigate cybersecurity incidents caused by various cyber threats. These have been prioritised in a suggested implementation order to assist organisations to build a strong cybersecurity defence for their systems.

The ACSC has also identified maturity levels based on the level of implementation of each mitigation strategy:

- Maturity Level One: partly aligned with the intent of the mitigation strategy
- Maturity Level Two: mostly aligned with the intent of the mitigation strategy
- Maturity Level Three: fully aligned with the intent of the mitigation strategy.

Once organisations have implemented their desired mitigation strategies to an initial level, they should focus on increasing the maturity of their implementation until they eventually reach full alignment (or a level that is appropriate and satisfactory for the organisation) for each mitigation strategy. The ACSC recommends that as a baseline, organisations should aim to reach Maturity Level Three for each mitigation strategy.

Mitigation strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Application Control	Application control is implemented on all workstations to restrict the execution of executables to an approved set. Application control is implemented on all servers to restrict the execution of executables to an approved set.	Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set. Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.	Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set. Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set. Microsoft's latest recommended block rules are implemented to prevent application control bypasses.

Mitigation strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Configure macro settings in applications such as MS Office	Macros are allowed to execute, but only after prompting users for approval. Macro security settings cannot be changed by users.	Only signed macros are allowed to execute. Macros in documents originating from the internet are blocked. Macro security settings cannot be changed by users.	Macros are only allowed to execute in documents from trusted Locations where write access is limited to personnel whose role is to vet and approve macros. Macros in documents originating from the internet are blocked. Macro security settings cannot be changed by users.
Restrict administrative privileges	Privileged access to systems, applications and data repositories is validated when first requested. Policy security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.	Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis. Policy security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.	Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis. Privileged access to systems, applications and data repositories is limited to that required for personnel to undertake their duties. Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.

Mitigation strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Multi-factor authentication	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smartcards, mobile app one-time password tokens, SMS messages, emails, voice calls or software certificates.	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smartcards or mobile app one-time password tokens.	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Multi-factor authentication is used to authenticate all users when accessing important data repositories. Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics or smartcards.
Daily backups	Backups of important information, software and configuration settings are performed monthly. Backups are stored for between one to three months. Partial restoration of backups is tested on an annual or more frequent basis.	Backups of important information, software and configuration settings are performed weekly. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for between one to three months. Full restoration of backups is tested at least once. Partial restoration of backups is tested on a bi-annual or more frequent basis.	Backups of important information, software and configuration settings are performed at least daily. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for three months or greater. Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur. Partial restoration of backups is tested on a quarterly or more frequent basis.

Mitigation strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Patch applications	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. An automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.
User application hardening	Web browsers are configured to block or disable support for Flash content.	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements. Web browsers are configured to block Java from the internet.	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements. Web browsers are configured to block Java from the internet. Microsoft Office is configured to disable support for Flash content. Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.

Mitigation strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Patch operating systems	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. An automated mechanism is used to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.

APPENDIX 2 UNACCEPTABLE USE OF COMPANY ASSETS

The following activities are strictly prohibited, with no exceptions:

- violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the company.
- unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the company or the end user does not have an active license is strictly prohibited.
- accessing data, a server or an account for any purpose other than conducting company business, even if you have authorised access, is prohibited.
- exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- introduction of malicious applications into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- using a company computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- making fraudulent offers of products, items, or services originating from any company account.
- making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- port scanning or security scanning is expressly prohibited unless prior notification to the IT Manager is made.
- executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- circumventing user authentication or security of any host, network or account.
- introducing honeypots, honeynets, or similar technology on the company’s network.
- interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- using any application/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- providing information about, or lists of, company employees to parties outside the company.

APPENDIX 3 SOCIAL ENGINEERING FRAUD COUNTERMEASURES

As with other cyber security threats, prevention is the best defence in minimising the risk of social engineering fraud. A proper countermeasure training program should include the following measures:

- Conduct a data classification assessment, identifying which employees have access to what types and levels of sensitive company information. Know who the primary targets of a social engineering scheme are likely to be. Remember, all employees are at risk.
- Never release confidential or sensitive information to someone you don't know or who doesn't have a valid reason for having it—even if the person identifies himself or herself as a co-worker, superior or IT representative. If a password must be shared, it should never be given out either over the phone or by email. Establish procedures to verify incoming checks and ensure clearance prior to transferring any money by EFT.
- Reduce the reliance on email for all financial transactions. If email must be used, establish call-back procedures to clients and vendors for all outgoing fund transfers to a previously established phone number, or implement a customer verification system with similar dual verification properties.
- Establish procedures to verify any changes to customer or vendor details, independent of the requester of the change.
- Avoid using or exploring "rogue devices" such as unauthenticated thumb/flash drives or software on a computer or network.
- Be suspicious of unsolicited emails and only open ones from trusted sources. Never forward, respond to or access attachments or links in such emails; delete or quarantine them.
- Avoid responding to any offers made over the phone or via email. This could include unsolicited offers to help to solve a problem such as a computer issue or other technical matter. If it sounds too good to be true, then it probably is.
- Be cautious in situations where a party refuses to provide basic contact information, attempts to rush a conversation (act now, think later), uses intimidating language or requests confidential information.
- Physical documents and other tangible material such as computer hardware and software should always be shredded and/or destroyed prior to disposal in any on-site receptacles, such as industrial waste bins.

- Proactively combat information security complacency in the workplace by implementing internal awareness and training programs that are reviewed with employees on an ongoing basis.
- Developing an incident reporting and tracking program to catalogue incidents of social engineering and implementing an incident-response strategy.
- Train customer service staff to recognise psychological methods that social engineers use - power, authority, enticement, speed and pressure. If it is important enough to move quickly on, it's important enough to verify.
- Consider conducting a recurring, third-party penetration test to assess your organisation's vulnerabilities, including unannounced random calls or emails to employees soliciting information that should not be shared.
- Guard against unauthorised physical access by maintaining strict policies on displaying security badges and other credentials and making sure all guests are escorted. Politely refuse entry to anyone 'tailgating'.
- Keep sensitive areas, such as server rooms, phone closets, mail rooms and executive offices, secured at all times.
- Monitor use of social media outlets, open sources and online commercial information to prevent sensitive information from being posted on the Internet.

APPENDIX 4 SOCIAL MEDIA GUIDELINES

Persons using company systems to access social media are required to adhere to the following guidelines at all times. Employees must not comment on or disclose confidential information about the company (such as financial information, current & future business performance, business plans, imminent departure of staff members) unless authorised to by management of the company.

Additionally, employees must ensure that:

- any content published is factually accurate and complies with relevant company policies
- they are not the first to make a Company announcement unless they have received the appropriate clearance from their manager
- they do not post material that is obscene, defamatory, threatening, harassing, discriminatory or hateful to another person or entity, including the Company, its employees, its contractors, its partners, its competitors and/or other business-related individuals or organisations
- they do not disclose other people's (i.e., clients) personal or work-related information
- are polite and respectful of others' opinions, even in times of heated discussion and debate
- they do not imply in any way that you are authorised to speak on the company's behalf
- they do not knowingly use the identity of another company employee or an employee of a company business partner or competitor (including name or variation of a name)
- they do not offer personal perspectives on a matter related to the company, and be mindful that any commentary and opinion on their part is not damaging to the company's reputation or commercial interests or bring the company into disrepute
- they always pause and think before posting.

Personal use of social media is not permitted during business hours and should only be accessed before and after the employees working hours and during the employee's work or lunch breaks. It is important to note that this policy does not apply to employees' personal use of social media platforms where the employee makes no reference to the company; however, employees must ensure that their use of social media on company systems does not breach the guidelines for unacceptable use of company assets in Appendix 2.