Information and Cyber Security Policy

Contents

Background 2
Purpose 2
Scope/application of the policy 2
Policy statement and principles 2
Protective cyber activities for staff 3
Protective cyber activities for elevated privileged accounts 3
Cyber Events or Incidents 4
Preventative Procedures 7
Roles and responsibilities 12
Review 14
Revisions made to this policy 14
Glossary of terms/definitions 14
Linked policies/procedures and/or forms 15
Appendix A: Cyber security incident or data breach action plan 20
Appendix B: Business Impact Analysis 22
Appendix C: Essential 8 Security Controls 24

Background

This policy outlines internal cyber incident response policies and procedures. It provides important information about the risk of cyber incidents to clients and the roles and responsibilities of staff when managing a cyber incident. Data breaches can cause significant harm in multiple ways. A data breach can negatively impact an entity's reputation for privacy protection. Compliance with the requirement to secure personal information in Australian Privacy Principle (APP) 11 is key to minimising the risk of a data breach. APP 11 requires entities to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Purpose

The purpose of this policy is to clearly define the roles and responsibilities for the investigation and response of cyber security incidents and data breaches.

The policy outlines the mandatory requirements to which all taff must adhere, to ensure cyber security risks to our information, network and systems are appropriately managed.

This Information and Cyber Security policy outlines:

- technology and information assets needs to protect
- threats to those assets
- rules and controls for protecting them

Scope/application of the policy

This policy applies to information systems, regardless of ownership or location, used to store, process, transmit or access data as well as all employees, including casual staff, contractors, those employed by contracted entities and others authorized to access enterprise assets and information resources.

This policy outlines the technology and information assets that need protection, possible threats to those assets and the rules and controls for protecting them and clients and business.

Policy statement and principles

We are committed to the protection of confidential information, our data and systems. This will be achieved by the implementation of measures across the systems and practices which maintain the confidentiality, integrity and availability of information held.

The following guiding principles underpin policy framework and incident response plans:

- Staff play a vital role in protecting the technology and information assets of the business.
- Staff have a clear understanding of the acceptable use of devices.
- Staff understand how to handle and store sensitive information and how to protect the organisation's information assets.

- IT Operations and other external service providers are accountable for protecting the ICT network and assets against the risk of cyber incidents, including the protection of client data.
- IT Operations and other external service providers remain responsive to changes in the cyber risk environment, ensuring current technology and security protocols are maintained.
- Responding in a collaborative and open manner with any affected parties before, during and after any cyber incident, to ensure ongoing improvements to the cyber security framework.

Protective cyber activities for staff

The following are the key outcomes identified as essential to a protective cyber stance:

- Password/passphrase requirements
- Multifactor authentication
- Email security measures
- Managing sensitive data
- Managing technology practices
- Standards for social media and internet access

Protective cyber activities for elevated privileged accounts

In addition to the staff responsibilities listed above, the following key outcomes must be met:

Password/passphrase requirements

Administrator passwords need to be:

- Complex, unique and unpredictable passphrases
- Frequent change of passwords
- Use of MFA

Email security measures include:

- As a warning banner on external emails as an additional warning to staff to be wary of malicious emails.
- Ensure email filtering services are maintained.

Managing Sensitive Data includes:

- Follow the Australian Privacy Principles and meets Australia data sovereignty requirements.

Cyber Events or Incidents

Cyber events or incidents response planning

- Implementation of an agreed cyber security incident or breach response plan
- Agree the critical business functions impacted (including the underlying systems and data)

Identification of potential incident

Category and Business Impact Level	**Description and Impact Statement**	**Notification Requirements**	**Triggers for escalation to a higher category**
Cyber security events Business Impact Level 0	A possible breach (or unconfirmed) cyber incident with no impact to systems or services	Consider notification to internal security representative Notification to Director	Substantial increase in cyber security alters, or continued cyber security alerts with potential to breach security controls
Cyber Incident Business Impact Level 1	An unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations Minor impact to services, information, assets, reputation or relationships	Notification to the Director	Actual or high likelihood: For limited or major impact to services, or To affect multiple organisations, or data breach
Significant Cyber Incident Business Impact Level 2 and 3	Successful compromise of security controls Limited or major impact to services,	Notification to the Director	A situation that: • has the potential to cause or is causing loss of life and

	information, assets, reputation or relationships A significant cyber incident is also any cyber incident that involves: • critical infrastructure or essential services; or • a data breach	Office of the Australian Information Commissioner*	extensive damage to property, infrastructure or • has the potential to have or is having significant adverse consequences
Cyber Emergency Business Impact Levels 4 and 5	Serious or exceptional compromise of security controls that: has the potential to cause or is causing extensive damage to information, assets, reputation or relationships has the potential to have or is having a significant adverse consequence for clients or the community	Notification to the Director Notification to any compromised owners of data Office of the Australian Information Commissioner* Notification to any appropriate law enforcement authorities	

Assessment of a potential incident

Staff will always be encouraged to report potential security concerns for assessment. If staff believe their device has been compromised:

- Disconnect from the network (i.e. remove network cable and disable WIFI).

In the case of a potential incident:

- Start investigation
- Continue to investigate the point of impact or cause of the incident, assess the impact, and review the appropriate data sources.
- Limit as much damage as possible by isolating any affected systems

- Put in place agreed containment strategies
- Repair and restore systems
- Complete any mandatory reporting requirements to appropriate authorities

Business Impact Level	**Description**	**Key Indicators and Consequences for Cyber Incidents**
N/A - Level 0	No business impact	No service impact
Minor – Level 1	Compromise of business information would be expected to cause minor harm to business operations	Compromise of the organisations non-critical physical or material assets. No threat to, or disruption of business operations, systems or service delivery. No damage to relationships between clients.
Limited – Level 2	Compromise of the information would be expected to cause limited harm/damage to business operations	Reputational damage or embarrassment Public concern or dissatisfaction. Degradation or cessation of non-critical (non-essential) business operations, systems or services, leading to the reduction in the efficiency and effectiveness of functions.
Major - Level 3	Compromise of the information would be expected to cause major harm/damage to business operations	Reputational damage or embarrassment Broad public concern or dissatisfaction. Degradation or cessation of critical (essential) business operations, systems or services, to an extent cannot perform one or more of its primary functions. Breach of personal information.
Serious - Level 4	Compromise of the information would be expected to cause serious harm/damage to business operations	Reputational damage or embarrassment for Widespread public concern or dissatisfaction. Degradation or cessation of critical (essential) business operations, systems or services, to an extent that cannot perform any of its primary functions. Breach of personal information.
Exceptional - Level 5	Compromise of information would cause grave damage to reputation	Grave reputational damage. Widespread public concern or dissatisfaction.

		Cessation of critical (essential) business operations, systems or services, to an extent that cannot perform any function. Breach of personal information. Notifiable incidents and potential legal action.

Post Incident Review

Post-incident review (PIR) is a detailed retrospective that allows an enterprise to carefully understand each part of an incident, from start to finish. It is one step in the incident response process that requires a cross-functional effort from all individuals and technologies connected to the incident to truly understand the root cause and full scope of the attack.

- Conduct a PIR and identify any necessary improvements or further required hardening of the security perimeter.
- Ensure response plan and policy documentation is updated and response changes advised to key positions and staff.
- Assess any impact and confirm containment strategy was effective

Preventative Procedures

Cyber incidents and mitigation strategies

While no single mitigation strategy is guaranteed to prevent cyber security incidents, organisations are recommended to implement eight essential mitigation strategies (The Essential Eight - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-explained) to make it much harder for adversaries to compromise systems.

Once implemented the below mitigation strategies to an initial level,
focus on increasing to the agreed maturity level.

IT Operations are responsible for planning and executing cyber attack exercises to validate response plans and remediate any identified gaps in security. External cyber specialists should be engaged on an annual basis to conduct a review of the environment, including penetration testing of business systems and applications.

IT Mitigation Strategies to Recover Data and System Availability	
Backups It is essential that most important data and information is backed up regularly. This should include: • daily incremental back-ups to a local storage device and then replicated off-site and cloud storage • regular testing that restoration of data from backups is achievable • ensure there are off site backups • ensure backups are not connected to active devices • ensure multi-factor authentication for access and recovery for backups Test restoration initially, annually and when IT infrastructure changes.	**Why:** To ensure information can be accessed following a cyber security incident (e.g. a ransomware incident).
IT Mitigation Strategies to Prevent Malware Delivery and Execution	
Application control to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers. • Limits application installation on devices. • More work to come regarding enhancing the Standard Operating Environment (SOE), Mobile Device Management (MDM) and Bring Your Own Device (BYOD) solutions to protect MH Data.	**Why:** All non-approved applications (including malicious code) are prevented from executing.
Configure Microsoft Office macro settings to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate. • Macros are disabled by default. However, users can manually overwrite to enable the macros	**Why:** Microsoft Office macros can be used to deliver and execute malicious code on systems.
Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.	**Why:** Security vulnerabilities in applications can be used to execute malicious code on systems.

• Internal IT and third party vendor to ensure patch management is done in regular cycle.	
User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers. • Level of group policy management in place.	**Why:** Flash, ads and Java are popular ways to deliver and execute malicious code on systems.
IT Mitigation Strategies to Limit the Extent of Cyber Security Incidents	
Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing. • All staff have a named user account. • Audits are carried out to confirm with compliance along with file\folder restrictions. • Administrators have separate named admin accounts for completing administrative tasks and so there is no cross over with the standard user account.	**Why:** Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.
Multi-factor authentication other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository. • For IT and Admin systems capable, IT utilise MFA for any systems that have the option to use MFA enabled. • Uses an Authenticator tool.	**Why:** Stronger user authentication makes it harder for adversaries to access sensitive information and systems.
(including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions. • Internal IT to ensure patch management is done in regular cycle.	operating systems can be used to further the compromise of systems.

Device and Network Security

The IT Operations Team, in conjunction with select third party vendors, are responsible for ensuring the operating system and security software patches are updated automatically. Updates contain important security upgrades for recent viruses and attacks, so it is important to complete updates promptly.

Internet Perimeter Security

All access from the network to the internet is secured via a firewall. All incoming and outgoing traffic must traverse the firewall. The firewall is set up to protect internal networks and portable business devices, and is regularly patched.

When connected to the internet off the network, staff need to ensure their internet and devices are patched and maintained. The systems are protected.

Anti-Virus Protection

Ensure protection software includes malware, anti-virus, anti-spyware and anti-spam filters.

All end user computers and corporate servers shall be secured from virus attack with the installation of an anti-virus software. This anti-virus software shall be kept up to date with regular patches and the latest virus software signatures.

Spam filters should be applied to help reduce the chances of opening a spam or dishonest email by accident.

Password requirements and Multi Factor Authentication (MFA)

- Business systems will require a password and a MFA code before access is granted.

Administrative privileges

To avoid unauthorised access to the environment:

- No generic credentials.
- Credentials must not be shared.
- All passwords to meet password complexity requirements.
- Keep number of admin accounts to operational minimum.
- Restrict access to accounts with administrative privileges.

- Regularly review the administrative accounts monthly.

User Access

All users who require access to the systems and network shall be allocated unique credentials which are governed by the policies detailed in this document.

For a new staff member to gain access to devices, systems and networks they must complete the confidentiality

Personal Drive

Each staff member's personal drive stores personal information relevant to their work

Storage and disposal

Use and disposal of computer equipment and systems

IT Operations are responsible for ensuring there is an updated asset register of devices and software, including accounts for internal systems and 'as a service' software that is used.

IT is responsible for ensuring the removal of any software or equipment that is no longer required, and that any retired devices are appropriately cleaned to ensure all data or sensitive business information is completely erased.

Device Data Storage

When disposing of hard drives they must be destroyed or formatted to ensure that all confidential information is completely removed and un-attainable.

Staff training and compliance

All staff must complete cyber security training. After completing the training, staff will be able to:

- Identify parts of an email that could indicate a hoax/phishing/scam;
- Describe the implications of using free email providers;
- Demonstrate how to protect personal information (privacy settings etc.);
- Identify how to share information safely and responsibly via social media;
- Demonstrate how to protect mobile devices and information;
- Recognise the factors that make up a strong password;
- Use strong passwords to keep safe online;
- Demonstrate how to identify trustworthy websites;
- Demonstrate how to ensure a safe browsing experience;
- Take appropriate actions when suspected or actual cyber-attacks occur.

Client Information

IT Operations are responsible for:

- a secure online environment for data capture or financial transactions
- security of any sensitive client information stored
- meet the Australian Privacy Principles in its management of client information
- meet all data management regulatory frameworks, both state and Federal

Cyber Security Insurance

ensure the appropriate level of cyber liability insurance cover is in place.

Protective cyber activities for staff

Password/passphrase requirements

A password is a string of characters that is used for authentication and access. Your password needs to be kept private so that unauthorised access to the computer system cannot be gained. Whenever you can, use a passphrase instead of a password. By following as many of these principles as you can, you will know you have created the most secure passphrase possible.

- ***Create complex passphrases*** - Complexity is defined as using a combination of different character sets: capital letters, lowercase letters, numbers and special characters. Combining character sets can make a passphrase more difficult to guess and increases the time it takes to be cracked. For example, ‘red House #sky tra1n’, ‘Sleep fr3e hard idea!’ or ‘crystal 0nion clay @Pretzel‘.
- ***Create unpredictable passphrases*** - The less predictable your passphrase, the better. A passphrase in the form of a lyric, quote or sentence, like '1don’tlikepine@ppleonPizza.’, use punctuation, which adds complexity. Using a random mix of unrelated words is far more unpredictable, and will produce a stronger passphrase.
- ***Create unique passphrases*** - Use a unique passphrase for every valuable account. Reusing a passphrase makes each account that uses it more vulnerable. This is particularly important for valuable accounts like email, financial accounts and those that store banking details. Often email addresses are reused as usernames to log into multiple accounts, and the accounts are often used to store valuable personal information, making your email account a valuable resource. If adversaries have cracked your passphrase, they will attempt to use it for every account they find that is associated with you, and even change your passphrase so that you can’t regain access to your accounts. One way that you can reduce the burden of having unique passphrases for every valuable account is to use modifiers for each one based on the service that it relates to. For example, ‘crystal onion clay @Pretzel faceb00k’ or ‘#insta crystal onion clay @Pretzel’.
- ***Frequent changes to passwords and passphrases*** - All Marathon Health passwords will expire after 90 days and must be changed within this timeframe.
- ***Protect and secure your passphrases*** – the use of password managers as a good cyber security practice. Having a unique passphrase for every valuable account may sound overwhelming; however, using a password manager to save your passphrases will free you of the burden of remembering which passphrase goes where.

The choice and responsibility of password managers is up to each staff member.

A lot of web browsers provide an in-built password manager. You might have noticed the pop-up window asking to store your password when logging into accounts. Password managers are also sold separately, however, quality and security may vary.

- ***Multi-factor authentication*** - One of the best methods to protect information and data is by enabling and enforcing multi factor authentication (MFA). All staff to utilise MFA on devices. MFA requires the user to have more than one form of identity to access data or a system. An example of one factor authentication is a password, an example of two factor authentication is a password and a pin. This allows for additional security because if someone has discovered your username and password, they will not be able to access the system without the pin.

Email security measures include:

Email security refers to various cybersecurity measures to secure the access and content of an email account or service.

Email security protects sensitive information within email communications, prevents phishing attacks, spear phishing, email spoofing, unauthorized access, and loss or compromise of one or more email addresses.

- When to use or share a business email address
- Opening email attachments from trusted contacts and businesses, and when not to
    - A warning banner on external emails as an additional warning to staff to be wary of malicious emails.
- Blocking junk, spam and scam emails
- Identification and appropriate management of suspicious emails

Managing Sensitive Data includes:

Sensitive data is confidential information that must be kept safe and only accessed by individuals who have been granted approved access.

Access to sensitive data should be limited through sufficient data security and information security practices designed to prevent data leaks and data breaches.

- Understanding when sensitive data can and can't be shared
- The storage, backup and the ability to recover sensitive data
- Ensuring appropriate information architecture and data structures
- Destruction of data when required
- Other guidelines in managing sensitive data are mentioned in these policies and procedures: .
- Follow the Australian Privacy Principles

Managing Technology practices:

- Data can only be stored on or within approved devices and/or systems.
- devices can't be used for activities that are illegal or deemed inappropriate.
- Understanding where devices, such as a business laptops and mobile devices, can be accessed away from the workplace.
- Storage of devices and management processes for loss or theft.
- Appropriate use of spam filtering tools.
- Locking of screens when computers are left unattended, including the requirement to have auto lock enabled on all devices.

- Protecting data on portable removable devices.
- Restrictions on the use of removable devices.

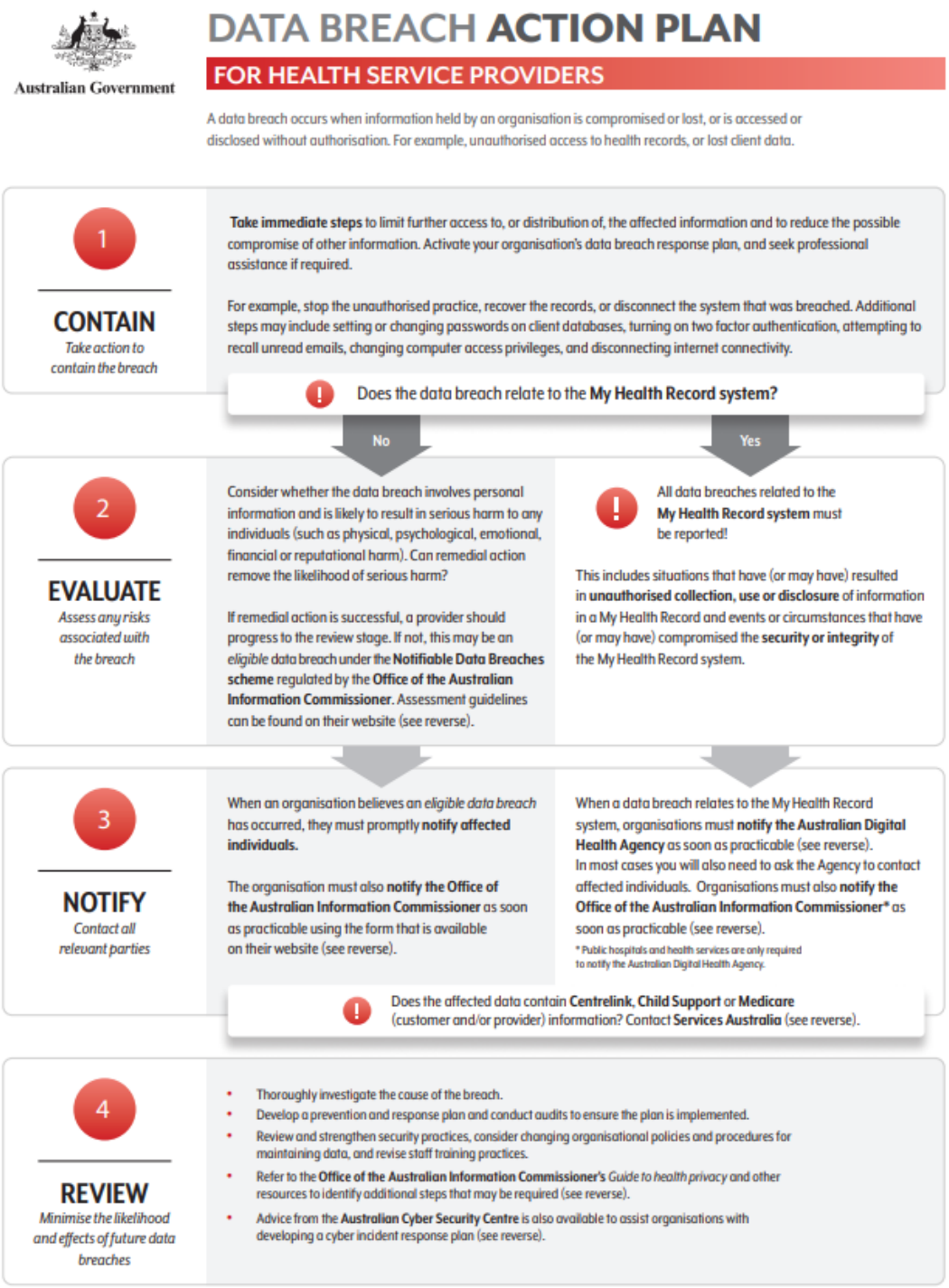
Standards for social media and internet access

- monitor internet usage and access.
- Understanding the appropriate use of social media when sharing business information.
- Agreement of use of the internet, including appropriate access to websites and social media platforms.

Appendix B: Cyber security incident or data breach action plan

A cyber security incident or breach response plan is a framework that sets out the roles and responsibilities involved in managing a data breach. It also describes the steps taken if a data breach occurs.

The immediate actions taken once a data breach is suspected or identified are crucial in minimising the harm that the data breach could cause. manage the process and follow these steps to manage a data breach when it occurs:



In addition to the steps above:

- **Document and Act –** Implement any additional actions that have been identified to mitigate risks. This could include actions such as initiating take down orders on external websites or putting processes in place to assist individuals who have been affected by the breach.
- **Prevent** – Put into action preventative efforts, based on the type and seriousness of the breach. This may include a security audit of both physical and technical security controls, a review of policies and procedures, a review of employee training practices or a review of contractual obligations with contracted service providers. If the breach has been reported to the Privacy Commissioner, further preventative and remedial actions may be recommended subsequent to the Privacy Commissioner's assessment. Update the cyber security incident response plan based on the lessons learnt so we can improve business response.

Appendix C: Business Impact Analysis

Governance		
Prepared by		Date
Plan Owners		
Critical Business Functions		
This plan covers the following functions: • Timing/description		
Authority for Invoking Plan		
A standing authorisation is given to the Plan owners to activate the Plan once confirmation is received from the EMT. Priority is given to Critical Business Function – Plan Owners are not to activate this Plan until confirmed.		
Business Impact Analysis		
Business Impact of Function loss	**Consequences of Non-delivery**	**Functional Interdependencies**
Current Resources / Premises / Equipment / Staff	**Minimum Resources Required**	**Alternate Manual Process or Work around**
Disruption Scenario		
Disruption Scenario		Maximum Acceptable Outage
Stakeholders / Communication Requirements		
Internal		External
Pre-event Preparedness (current policies and process and access points required to deliver function)		
Electronic copies		Hard copies
Emergency, Continuity and Recovery Response		
1. Manager to be advised 2. Key Decision makers to confirm expected downtime 3. Identify availability and coordinate required staff – in the event of loss of staff, the director is to be informed of temporary staff required to assist 4. Consult with internal and external stakeholders		

5. Identify and implement emergency response process – this may include identified alternate manual processes or work arounds 6. Document emergency response process taken and authorisations provided 7. Post event – review emergency response process and this sub plan and amend as required.		
Critical Staff contacts		
Contact	Contact details	Purpose/speciality
Key Internal / external contact		
Contact	Contact details	Purpose/speciality
Alternate Accommodation		
First option facility	Room no / location	Access arrangements / key holder
<u>Working from Home</u> This critical business function can be performed from an offsite location.		

Appendix D: Essential 8 Security Controls