



CITY OF
Port Adelaide Enfield

CITY OF PORT ADELAIDE ENFIELD CYBER SECURITY MANUAL

This manual should be read in conjunction with:

3.04.08 Cyber Security Governance Policy

3.04.09 Information Technology Use Policy

CONTENTS

CONTENTS.....	2
1. PURPOSE.....	5
2. SCOPE.....	6
3. ROLES AND RESPONSIBILITIES.....	7
4. END USER SECURITY	8
Training and Awareness	8
Personnel Onboarding and Exit	8
Information Asset Provision and Ownership	8
Password Management	9
Multi-Factor Authentication	9
Workstations and Work Areas.....	9
IT Equipment Care and Handling.....	10
Removable Media and Mobile Devices.....	10
5. ACCESS TO INFORMATION.....	11
Account Management	11
Privileged Account Management	11
Generic/Shared Accounts	12
Centralised Identity Management	13
Emergency Access (Break Glass) Accounts	14
6. ASSET IDENTIFICATION AND CLASSIFICATION	15
Asset Identification and Classification.....	15
Handling of Assets and Information	15
Information Labelling.....	16
Asset Provisioning.....	16
Confidential Council Reports	16
Asset Disposal	16
7. ICT SYSTEMS AND OPERATIONS	18
Change Management.....	18
System Resilience and Digital Preservation	18
System Configuration and Hardening	19
Network and Infrastructure Management.....	19
Firewalls	19
Wireless Networks	20
Remote Access	20
IT System Baselines	20
Server Baselines	21
Microsoft Office	21
Mobile Devices Baseline	21
Secure Logon Standards	21
Mobile Device Mangement.....	21
Logging and Monitoring.....	22
Vulnerability Management.....	22
Patching of Applications and Operating Systems	22
8. INCIDENT MANAGEMENT	24
Roles and responsibilities	24
Cyber Security Incident Response Management.....	24
Response Planning	25
9. THIRD PARTY MANAGEMENT.....	26
Third Party Security Compliance	26
Third Party Services Assessment	26

Third Party Maturity Assessment	26
Service Assessments	26
10. SYSTEM ACQUISITION AND DEVELOPMENT	27
System Design and Planning	27
Software Development	27
<i>Development Environment</i>	27
11. FACILITIES SECURITY	29
Site Categorisation	29
Facilities Security	29
<i>Employee Access</i>	29
<i>Equipment Security</i>	29
<i>Environmental Security</i>	29
DOCUMENT CONTROL.....	31
Annual Evaluation and Review	31
Related Information.....	31
Ownership and Approval.....	31
Version History	31
APPENDIX A - ASSET CLASSIFICATION STANDARD	32
Confidentiality.....	32
Integrity.....	33
Availability	34
Information Asset Handling Guidelines.....	34
APPENDIX B - PAE PASSWORD STANDARD	36
APPENDIX C - PAE ACCOUNT NAMING STANDARD	37
APPENDIX D - SECURE LOGON STANDARDS.....	38
APPENDIX E - INFORMATION SECURITY INCIDENT MANAGEMENT	39
Definitions.....	39
Governance Structure	39
Director, Corporate Services.....	39
Information Security Information Incident Response Team	39
Response Activities.....	40
Communication	41
Internal Communication of Information Security Events.....	41
Internal Communication During an Information Security Event	41
External Communication	41
Incident Response Framework ('ISIRF')	42
Process Overview	42
1. <i>Planning and Preparation Phase</i>	44
2. <i>Identification</i>	44
3. <i>Containment and Eradication</i>	44
4. <i>Post Incident Review</i>	44
Lessons Learned.....	45
Post Incident Reporting.....	45
APPENDIX F - SPECIFIC INCIDENT RESPONSE PROCEDURES	47
APPENDIX G - ICT STANDARD OPERATING PROCEDURES.....	53
Access Administration Procedures	53
Access Management.....	53
System Provisioning.....	61
Vulnerability Management.....	61
APPENDIX H - PROJECT AND CHANGE MANAGEMENT GUIDELINES	62

Project and Change Types.....	62
Project and Change Management Requirements.....	62
Major Projects and Changes.....	62
Moderate Projects and Changes	63
Incidental or Minor Changes	63
Emergency Changes.....	63
APPENDIX I - BACKUP AND DATA PRESERVATION.....	65
Daily Backup Checks	65
System Recovery Procedures.....	65
System Recovery Procedures.....	65
APPENDIX J - SECURITY ZONES.....	66
APPENDIX K - SOFTWARE DEVELOPMENT	68
Secure Development, testing and Deployment.....	68
System Design and Planning.....	68
Software Development.....	68
<i>Development Environment</i>	68
Secure Coding Standards	69
APPENDIX L - PROCUREMENT PROCEDURES.....	70
Contract Specification Guidelines.	70
APPENDIX M - SOURCES OF PRECURSORS AND INDICATORS.....	71
APPENDIX N – WORK INSTRUCTION ENROLLING SYSTEM USER.....	74
Checklist for creation of new user	89
Checklist for SEPERATION OF user	90
APPENDIX O – WORK INSTRUCTION ACCESS REVIEW	91
APPENDIX P – IT OPERATIONS START OF DAY CHECKLIST (BACKUPS, SERVERS, AND APPLICATIONS)	95

1. PURPOSE

The purpose of this Cyber Security Manual is to define the City of Port Adelaide Enfield's (PAE) control requirements to manage its cyber security risks.

This manual supports the PAE Cyber Security Governance Policy and is written to be consistent with the South Australian Cyber Security Framework ('SACSF').

2. SCOPE

This manual encompasses all personnel who have access to, are responsible for managing, or are users of PAE information assets.

The requirements and expectations outlined in this manual apply equally to all users of PAE assets, including:

- PAE employees;
- Contractors engaged by PAE;
- Volunteers appointed by PAE; and
- Suppliers providing services who may have an impact on PAE's cyber security.

It is mandatory that all users, whether directly employed, contracted, or otherwise authorised to use PAE information assets, comply with the directives of this policy.

Users of PAE's information assets are reminded that:

- Nothing in this policy or its supporting procedures and documents overrides an article of Law;
- Unauthorised actions may be subject to prosecution under national, state and local statutes, and such actions may involve law enforcement and/or legal action;
- All intellectual property and licensing requirements must be complied with; and
- Breach of any PAE policy may result in disciplinary action up to and including dismissal and/or the involvement of law enforcement.

3. **ROLES AND RESPONSIBILITIES**

Role	Responsibility
Executive Leadership Team	Approval of Information Technology Administrative Policies
Cyber Security Working Group	Provides oversight and guidance on the implementation of the controls documented in this manual. Ensure the manual has been adequately reviewed and approves its use.
Corporate Information Manager	The provision and implementation of IT systems, equipment, and information assets that support the objectives and processes outlined in this manual.
Information Asset Owners	Authorise access to information assets. Classify their information assets appropriately. Manage risks relating to those information assets.
Directors, Managers and Team Leaders	Fostering a cyber security conscious culture in their team by understanding the cyber security risks to their team, and encouraging the correct cyber security behaviours Ensuring training is provided to employees in positions of trust or who have heightened cyber security responsibilities, or increased risk profiles, to ensure sound cyber security practices are understood, and effective cyber security controls are implemented and followed. The proper induction of new users, and to ensure that all personnel in their area are made aware of IT Policies and this manual. Ensuring that suppliers are made aware of their responsibilities as outlined in this manual.
Users	Maintain a working understanding of and follow PAE's cyber security controls.

4. END USER SECURITY

The purpose of this section of the Cyber Security Manual is to ensure that all PAE personnel use PAE information technology ('IT') and information assets in an appropriate and responsible manner.

Procedures are in place to protect both personnel and PAE from inappropriate use of information and supporting IT assets that may expose the Council to risks resulting from the compromise of computing, telecommunications, networks, and information systems.

IT security is dynamic by nature and because of this PAE IT staff will exercise discretion in the application of required security measures to ensure PAE's IT systems are kept safe and secure, provided they are in line with the principles outlined in this manual.

TRAINING AND AWARENESS

All personnel including 3rd party service providers who have access to PAE information assets must be made aware of their information security responsibilities, security procedures, standards and guidelines.

Cyber security education and awareness training must be provided to all personnel and service providers during induction and at least annually thereafter, ensuring they are aware of their responsibilities regarding the appropriate use of PAE information assets

Additional security training must be provided to PAE personnel who are in positions of trust, have heightened security responsibilities, or have increased risk profiles (e.g., Privileged account holders, senior management, Information Security Incident Response Team (ISIRT) members)

PAE managers must ensure personnel and service providers responsible for cyber security management and day-to-day operations maintain industry recognised certifications relevant to their role, that have ongoing continuing professional education requirements or have been obtained within the previous five years.

PAE managers must evaluate the performance of all personnel with reference to cyber security responsibilities and performance requirements.

PERSONNEL ONBOARDING AND EXIT

All employees and third parties contracted by PAE or granted access to PAE information assets must be screened using appropriate background checks as described in the *Recruitment and Selection Policy 3.01.24*.

Responsibilities and duties valid after a change to, or cessation of employment must be documented in the employment or engagement contract.

Separating employees and volunteers must be made aware of their ongoing cyber security obligations and have their access to resources withdrawn as per Appendix G – User Access Removal Procedure.

Upon cessation of employment or engagement, all information assets must be returned in a timely manner and all access rights will be revoked within 8 business hours of the receipt of the separation form.

INFORMATION ASSET PROVISION AND OWNERSHIP

PAE provides and/or allows devices to be used to access the company's information, systems, software, facilities, and services. Upon ceasing employment or on contract

cessation with PAE, all PAE assets must be returned with their confidentiality and integrity maintained.

Information and information systems are open and available to PAE employees, subject to the controls needed to protect confidentiality required by legislation, employee privacy and the cost effectiveness of providing the information.

Access to information system functions and services may be restricted to provide necessary segregation of duties and control over data maintenance functions.

PASSWORD MANAGEMENT

All PAE account holders are responsible for adhering to the following password requirements.

- Passwords must meet the requirement of PAE's password standard
- Users must use a separate, unique password for each of their work-related accounts.
- Users must not use any work-related passwords for their own, personal accounts.
- Privileged accounts must have a unique password from all other accounts held by that user.
- Passwords must not be shared with anyone, including supervisors and co-workers, unless specifically required for use with shared accounts.
- Passwords must not be inserted into email messages, or other forms of electronic communication, nor revealed over the phone to anyone.
- Passwords must not be written down on paper or stored in an unsecured file, however passwords may be stored in an approved Password Manager.

Self-service password resets and account unlocking (using PAE provided tools) is encouraged

MULTI-FACTOR AUTHENTICATION

Multi-Factor authentication is a security measure that requires two or more proofs of identity to grant access to a resource. It provides additional assurance of user's identity and is one of the most effective ways to prevent unauthorised access to information assets. Multi-factor authentication must be enforced when user's are:

- Remotely accessing PAE resources (e.g VDI)
- Administering Cloud services
- Using privileged accounts to administer systems.

WORKSTATIONS AND WORK AREAS

Access to PAE premises is physically controlled and granted to employees on an as-needs basis. All employees are responsible for ensuring the following:

- Employees accessing 'RESTRICTED' areas are responsible for monitoring the work areas to ensure that no unauthorised individuals are present and/or unescorted;
- Visitors must be escorted by a PAE representative whilst in 'RESTRICTED' areas;
- All individuals present in 'RESTRICTED' areas must wear a form of visible identification;
- Workstations will be locked after 15 minutes of inactivity.
- Users must always maintain clear and tidy work areas.
- Information classified as 'RESTRICTED' must be stored in a locked drawer or cabinet when not in use;
- Whiteboards must be cleared of 'RESTRICTED' information when no longer in use.

IT EQUIPMENT CARE AND HANDLING

IT equipment is assigned to individuals to support their role. It is required that:

- Equipment is not marked or labelled by the user
- Identification labels are not removed
- Due care is taken with handling, storage and use
- Equipment is adequately secured to prevent theft, loss or damage
- Repairs and maintenance are only undertaken by repairers approved by the IT Section
- Stolen equipment reports are made to the Police and Governance/Insurance by the individual to whom the asset was assigned
- Equipment is not removed, swapped or taken home without notification to the IT Section

REMOVABLE MEDIA AND MOBILE DEVICES

- Portable storage devices from an untrusted source (e.g., found USB drives) or personal storage devices must not be connected to PAE equipment;
- Portable storage devices containing 'RESTRICTED' information must be stored in a locked drawer or cabinet when not in use.
- Portable devices must be physically secured and out of sight when unattended;
- Information stored and/or transported on portable devices must satisfy the relevant requirements as defined by their classification; and
- Laptops, mobile phones, and tablets used to connect to PAE systems (including personal devices) must be secured with an inactivity timer lock and a passcode.

5. ACCESS TO INFORMATION

The purpose of this section is to define the approach for managing user access to PAE systems, equipment and information assets ('IT assets') to prevent unauthorised access, and to ensure that effective controls are in place so that all users and their actions can be uniquely identified. PAE personnel and 3rd party service providers may be issued one or more of the following accounts:

- Standard account with limited access and privileges used for day-to-day work
- Privileged accounts used for administering systems or accessing sensitive information
- Shared Accounts used to access shared devices where credentials are known to multiple people.

The following sections define the requirements associated with each account type.

ACCOUNT MANAGEMENT

A formal user registration and access provisioning process must be followed to assign or revoke access rights to PAE IT assets. Standard User access to PAE IT assets must be:

- Assigned using the principle of least privilege (i.e. the minimum level of access required to fulfil the user's duties) and have a justified purpose;
- Assigned only after approval for the access is provided by the relevant manager or information asset owner;
- Uniquely identifiable and accountable to a single individual;
- Reviewed and revalidated at least annually
- Removed no later than eight hours from receiving the separation form when it is no longer required, e.g., upon termination of employment or contract, or adjusted upon change to their job function.

PAE user account administrators are responsible for managing account information as follows:

- Accounts must be named according to PAE's account naming standard as per Appendix C – PAE Account Naming Standards
- User identities must be positively verified before performing passphrase resets for user requests made remotely;
- Requests for passphrase resets from anyone other than the user of the account must only be accepted from CEO, Directors and Managers
- Users must be allocated a unique passphrase which must be changed upon first logon;
- Users must be provided their passphrase using a secure passphrase distribution process

PRIVILEGED ACCOUNT MANAGEMENT

In addition to the requirements for standard account management, privileged accounts must be managed as follows:

- Privileged accounts must only issued to individuals authorised by the Corporate Information Manager
- Where such privileged access is no longer tied to a valid business need, it must be revoked immediately.
- A review of privileged user access must be performed at least every 6 months.

- A separate administration account to the user's regular account must be assigned to personnel administering PAE information assets;
- Privileged accounts must not be used to access email, web-browsing or file downloading functionality.
- Privileged accounts must not be used to perform day-to-day activities.
- Privileged accounts must be subject to additional logging and monitoring for unusual activity.
- Multi-factor authentication is required to authenticate privileged users.

GENERIC/SHARED ACCOUNTS

In some situations, is it not practical or possible to assign a named account in accordance with PAE's account naming standard. In such cases a generically named, shared account may need to be assigned to a group of users who each know the credentials. Due to the increased risk associated with generic shared accounts, they must not be used unless absolutely necessary and where explicit approval has been obtained.

To reduce the risk associated with generic shared accounts passphrases on any shared administrative and/or service accounts must be changed immediately upon termination of employment or contract of any individual who has knowledge of that passphrase. A record of all passphrase reset requests must be retained in Fresh Service.

The following table details the specific requirements that must be applied to various types of generic shared accounts in addition to the directives already applicable to standard accounts.

Account Type	Requirements
Volunteers	a) Volunteers will have individual accounts – generic or shared accounts will only be provided when authorised in writing by the relevant Manager or Director. b) Volunteers will only have access to specific shared folders unless authorised in writing by the relevant Manager or Director. c) Volunteers will not have access to corporate systems unless authorised in writing by the relevant Manager or Director.
Front Counters	a) PAE Library Front counter workstations will have: i. minimum network access ii. maximum security imposed on them with regard to the systems they access iii. no connection to email iv. no administrator rights to any computer systems v. access to workgroup directories b) Any computers located at front counters or within public areas will have appropriate security systems (physical and logical) so as to maximize protection of those systems from unauthorised access. c) Passwords for public access will only be held by IT and nominated support staff (sponsors) within each area.

Work Experience Note: A work experience student is defined as a person engaged via a Workplace Learning Agreement form (typically from Secondary Schools, TAFE's and Universities) and have a placement period of less than 10 working days.	Work Experience students are not normally provided with a login. If access to a PC is required and approved in writing by a Manager or Director, a restricted login may be provided following a request via People and Culture. The restrictions shall be: • Limited access to network drives - no access to workgroup drives (G drive) • No access to external email • No access to the Internet • No access to corporate applications Work Experience students provided with a login are required to follow the procedure for incepting new users as below.
---	---

External Access	a) PAE may provide users and approved service providers with external access to Council systems subject to approval of the line Manager/Director and Corporate Information Manager. b) The preferred method of access is via a Virtual PC or Teamviewer with MFA enabled. c) Users and approved service providers may be given a tailored list of applications that is consistent with their security profile and/or approved requirement. d) If PAE's IT equipment has been used on an external network (e.g. a PAE Laptop on a home network) the equipment is not be connected to the PAE's network until it has been deemed virus free by IT staff.
Field Staff Access	a) With the exception of field staff who act as a Field Team Leader or have access approved by a Director or Manager, field staff have no direct access to the Windows Network. b) The preferred method of accessing an application is via the Microsoft Azure AD login with MFA enabled. c) Note: Employees may be users in Microsoft Azure AD without having any other licenses.

CENTRALISED IDENTITY MANAGEMENT

Authentication should be integrated with PAE's Active Directory in preference to creating new users and security groups local to a service or device. This approach consolidates account management to a central location thereby reducing administrative effort relating to account onboarding, termination and audit. It also reduces the number of credentials personnel are required to remember.

Where Active Directory integration is not supported, a local account must be created and managed in accordance with PAE's account and password requirements as described in this manual.

Where Active Directory integration is implemented it is important to ensure an alternate, non-domain based method of emergency administrative access is available.

EMERGENCY ACCESS (BREAK GLASS) ACCOUNTS

All systems should be able to be accessed via an emergency account where access cannot be gained via the normal authentication process (e.g misconfiguration error, Active Directory Outage). An emergency access account is typically a local system user which is not dependant on external authentication and may be either in-built or specifically created. Emergency Access accounts are typically highly privileged and not associated with a named user and therefore present an increased risk to PAE. Particular care must be taken to protect these accounts.

Emergency Access Accounts must be managed as follows.

- Credentials should be stored and secured by a PAE custodian (e.g system owner) and not be shared with other parties except when required for testing or emergency access.
- Credentials should be changed by the custodian after use, to restore confidentiality.

6. **ASSET IDENTIFICATION AND CLASSIFICATION**

Information assets supporting critical processes must be identified, recorded and classified. PAE defines several sensitivity classifications each with differencing handling requirements. This section specifies, how information can be shared with other organisations and individuals, and what level of permission needs to be obtained prior to disclosing information to an external organisation.

The South Australian Cyber Security Framework defines an Information Asset as, “*Any information or asset supporting the use of the information that has value to the agency, such as collections of data, processes, ICT, people and physical documents.*”

When an information asset is procured, obtained, or created it must be:

- Formally assigned an owner.
- Classified
- Recorded in an information asset register if it supports critical PAE processes.

All users handling PAE information assets must follow the relevant processes for labelling, storing, handling and disposing of assets in alignment with their classification. These processes are detailed in *0 - Information Asset Handling Guidelines*. Information asset owners are responsible for ensuring relevant handling processes are documented and followed.

ASSET IDENTIFICATION AND CLASSIFICATION

An inventory of information assets associated with information and information processing must be maintained with the following details recorded:

- Asset identifier, name and type;
- Asset owner;
- Asset location; and
- Asset classification ('CIA').

PAE information assets are to be classified as defined in *Appendix A – Asset Classification Standard*

It is important to note that there can be an aggregated effect to data classification, for example:

- Information records such as archives will contain various records and are therefore likely to contain information with varying classifications;
- IT assets are likely to contain information of varying classifications; and
- Communications links can transmit data of varying classifications.

Data repositories and applications must be handled according to the requirements of the highest classification of data held or transmitted.

HANDLING OF ASSETS AND INFORMATION

All PAE staff and external providers must handle information assets in accordance with the following:

- Unclassified information obtained from outside PAE must be handled according to PAE's classification scheme;
- The recipient of information obtained from outside PAE that is clearly labelled with an external classification must ensure that the handling requirements of that data are understood and applied as expected;

- Any information classified as 'RESTRICTED' or higher must not be shared with anyone who is not employed or engaged by PAE unless a non-disclosure agreement is in place that specifically details the obligations of the involved party/parties to protect the information;
- Physical assets with a classification of 'RESTRICTED' must be physically secure or under the personal control of a PAE employee at all times;
- Physical assets with a classification of 'RESTRICTED' or higher must be stored out-of-sight when not in use;
- Fixed assets (e.g., servers) must not be taken off-site without prior authorisation; All assets are to be properly maintained. This includes any preventative or scheduled regular maintenance.
- Information must not be provided to any person or organisation that does not have a legitimate business reason to have the information.
- Information must not be saved for non-PAE use

INFORMATION LABELLING

The default confidentiality classification level for all information assets is INTERNAL. Any asset without an explicit label must be considered INTERNAL and handled as such.

The following principles apply with respect to information labelling:

- Information classified as 'RESTRICTED' must be clearly labelled;
- Information classified as 'RESTRICTED' must be clearly labelled if it is to be shared with a third-party;
- The information asset owner is responsible for controlling reclassification of the information; and
- Information assets must not be reclassified without written approval from the asset owner.

ASSET PROVISIONING

IT information assets are assigned to individuals to support their role. It is required that:

- Details of any assets issued to employees or contractors are recorded in the relevant asset inventory (Fresh Service);
- Individuals issued with assets are made aware of their responsibilities with regards to the appropriate care and protection of these assets;
- At the time that an asset is no longer required by an individual it must be reclaimed;
 - Specifically, at the cessation of employment, or at the end of a contract or assignment, all assigned assets must be reclaimed from the relevant individual; and
- The asset inventory will be updated reflecting returned or disposed assets.

CONFIDENTIAL COUNCIL REPORTS

Confidential Council reports will be managed separately as per the established process and will include a 'Confidential' watermark.

ASSET DISPOSAL

All PAE information assets must be disposed of in a controlled manner to ensure confidentiality is maintained.

- Assets awaiting destruction must continue to be handled according to their classification. They must be clearly marked as awaiting disposal and held in appropriate storage until sent to a facility for destruction;
- Hardware assets must be checked to validate that all 'RESTRICTED' data has been removed or destroyed from internal storage disks;
- Media that cannot be effectively sanitised must be destroyed so that data is irrecoverable;
- Approved third-party hardware disposal facilities must be used for 'RESTRICTED' hardware;
- A clear record of authorisation and handover, and a certificate of destruction must be retained as long as required to meet all legal, regulatory and business requirements;
- Disposal of IT assets must comply with environmental guidelines; and
- The asset inventory must be updated reflecting returned or disposed assets.

7. ICT SYSTEMS AND OPERATIONS

Standard operating procedures and technical controls must be in place to provide a consistent and secure approach to systems' administration, maintenance and configuration activities. This must include:

- The development and use of standard operating procedures (SOPs) for primary cyber-security functions.
- The implementation of formalised change management procedures
- The implementation of appropriate system redundancy commensurate with each systems availability requirements
- The implementation of appropriate backup procedures and periodic recovery testing.
- Centralised logging and retention of events to facilitate incident detection and analysis.
- System hardening in commensurate with each system' s risk exposure.

Operational responsibility for managing the communications network, systems and services supporting PAE information assets must be established and documented.

CHANGE MANAGEMENT

PAE Managers and system owners must take steps to identify, understand and manage Information Security risks associated with system changes that align with PAE's risk appetite.

- A risk assessment must be documented for all projects undertaken by PAE
- All changes to PAE information assets must be documented and approved before implementation in accordance with PAE's change management procedures detailed in **Appendix H - Project and Change Management**

SYSTEM RESILIENCE AND DIGITAL PRESERVATION

Maintaining availability of key systems and services is critical to day-to-day operations at PAE. Consideration needs to be given to the redundancy of critical service to ensure they are robust enough to withstand planned or unexpected failures. Backups of systems and information must also be in-place to reduce the risk of data loss and adhere to legislated data retention requirements.

Recovery objectives for PAE systems and services must be documented as part of a business impact assessment with appropriate measures then taken to implement and test redundancy and backups. A backup and restoration strategy must be implemented to support business continuity requirements as defined within the *Business Continuity Plan and Incident Management Procedures*.

Backups of important information, software and configuration settings must be performed daily, with backup information:

- Retained for a period of at least two years, in alignment with State Records requirements;
- Stored in a non-rewritable and non-erasable manner; and
- Stored at multiple geographically dispersed locations.

A backup monitoring process must be defined that details how backup failures are logged, investigated, and tracked. The backup and restoration strategy must be tested quarterly. Additionally, a full system restoration test must be performed at least once when a system is initially implemented, and each time a substantial infrastructure change occurs thereafter.

System owners must ensure detailed business continuity plans are implemented to enable PAE to maintain key operating capabilities in the event of a system failure. These plans must consider information security requirements for critical systems.

SYSTEM CONFIGURATION AND HARDENING

When systems are deployed in their default state it can lead to an insecure operating environment which may leave them vulnerable malicious or inadvertent attack. Vulnerable systems will assist an adversary to gain a foothold in, and traverse through an environment. Most systems can be configured in a more secure state to minimise this security risk.

Hardened Standard Operating Environment (SOE) definitions for PAE systems (e.g Workstations, Servers, network devices) help to ensure a consistent and secure baseline is applied across the environment. Where appropriate SOE's should be developed, maintained and implemented for PAE systems taking into account:

- The risks associated with particular systems
- The expectations of the SACSF
- Vendor guidance and best practise
- Specific PAE requirements described within section 0

NETWORK AND INFRASTRUCTURE MANAGEMENT

The following principles must be adopted for PAE networks and IT infrastructure:

- PAE information passing across public networks must be protected from compromise commensurate with the classification of the information;
- Groups of information services, users and information systems must be segregated throughout the IT environment to limit damage in a situation where one environment is compromised;
- All network infrastructure and system changes must be managed under change control as described in the *Project and Change Management Section of this document*;
- Administrative personnel responsible for maintaining network infrastructure and systems should possess the appropriate skills, training and where possible relevant certifications;
- Installation of software on operational systems must be managed through change management, with access to perform such changes restricted to administrative users only;
- Proactive and regular system capacity planning of core systems must be performed to ensure the adequacy of processing and storage capabilities; and
- The network must be monitored (e.g., with alerting rules) for signs of malicious activity.

FIREWALLS

The following directives apply with respect to firewalls:

- Firewalls must be managed from the most secure side (e.g. from the internal network);
- Firewall rule sets must be reviewed on an annual basis or after major changes in the network architecture;

- Firewalls must be configured with intrusion detection capabilities to inspect all traffic passing through them, and regularly updated with signature files of known vulnerabilities / attack patterns.

WIRELESS NETWORKS

The following directives apply with respect to wireless networks:

- All wireless access points connected to the PAE network must be approved by the Corporate Information Manager prior to installation;
- A 'guest' network may be maintained which provides non-PAE devices access to the internet;
- All wireless communications between PAE devices and networks must be encrypted; and
- Wireless access points must be periodically scanned for vulnerabilities and the existence of unauthorised access points.

REMOTE ACCESS

All remote access to the PAE IT environment must be configured to use the Virtual Desktop Interface ('VDI') capability or a PAE licensed Teamviewer account.

IT SYSTEM BASELINES

All information technology systems owned and/or managed by PAE must be vendor supported, kept up-to-date and secured with:

- Supported operating system and application patches;
- Local firewall; and
- End-point protection software updated from a centralised console.

All PAE information technology systems must align with the following standard configuration requirements:

- Access to PAE devices and systems must only be granted upon successful authentication.
- Unnecessary operating system services or features must be disabled;
- Systems are secured using vendor security recommendations;
- Remote management access must be configured so that only designated management workstations and networks can connect to the device;
- Insecure protocols such as Telnet and FTP must be disabled, or protected by other secure protocols such as IPsec or SSL/TLS as required;
- Web browsers must be configured to block or disable Flash content, Web Advertisements, and Java from the internet.
- Functionality that automatically executes code on removable media must be disabled, e.g. Windows autorun;
- User sessions must be configured to time out and lock after 15-minutes of inactivity;
- Security monitoring agents must be installed and configured where available;
- Local accounts must be configured to meet passphrase requirements as defined in Appendix C – Account Naming Standards; and
- Default vendor credentials must be changed.

Standard user accounts must not have the ability to reconfigure the defined IT system baselines.

SERVER BASELINES

In addition to the IT System Baselines described above, servers hosted in environments operated and managed by PAE must meet the following requirements:

- Production and non-production environments are segregated;
- Console/interactive access and local administrator access is limited to authorised users with a defined business need;
- Monitoring tools must be configured to identify unauthorised changes to IT assets; and
- System clocks must be synchronised to a single reference time source or local standard time.

MICROSOFT OFFICE

Where Microsoft Office is installed the following steps must be taken to reduce the vulnerable attack surface:

- Only signed Microsoft Office macros can execute,
- Microsoft Office macros in documents originating from the Internet are blocked, and
- Microsoft Office macro security settings cannot be changed by users.

MOBILE DEVICES BASELINE

In addition to the IT System Baselines described above, mobile phones and tablets must meet the following requirements:

- Mobile devices connecting to PAE information systems must be from an approved fleet;
- Mobile devices are only used to access information of classification up to 'RESTRICTED' unless configured with a Mobile Device Management agent; and
- Mobile devices must be configured to automatically lock, and require authentication such as facial recognition, fingerprint scan or a pin code to unlock.

SECURE LOGON STANDARDS

PAE information assets must be configured to meet the secure login standards defined in Appendix D – Secure Login Standards.

MOBILE DEVICE MANGEMENT

PAE staff may use laptops and other mobile devices to remotely access PAE information assets. A mobile device management solution must be in place to ensure appropriate controls are applied to all mobile phones, including personal phones used for work. The following controls must be applied to mobile devices accessing Council information:

- Passphrases or passcodes must be required to access the device
- Encryption of storage is enabled for laptops, mobile phones, and removable storage devices
- Remote wipe functionality is in place to allow Council data to be removed from remote devices.

- Processes must be in place to request and authorise the use of personal devices to access Council information (e.g. emails)
- MFA must be enforced during the initial configuration of access to PAE email, and whenever an account password is changed.
- Remote working procedures and cybersecurity guidance must be socialised with PAE personnel and contractors working offsite.

LOGGING AND MONITORING

Appropriate logging and monitoring capabilities must be implemented to identify and alert on suspicious IT system and network activity and/or provide evidence of activities to be used during incident response.

- Logs must be captured and stored centrally, and protected against unauthorised access and tampering;
- Logs must be retained for at least 18 months;
- Event logs recording user activities, exceptions, fault, and information security events must be captured and reviewed based on an assessment of risk; and
- All activity by administrative users must be captured.

VULNERABILITY MANAGEMENT

A threat and vulnerability management program must be in place to detect and remediate technical vulnerabilities.

- External sources (e.g. AusCERT feeds, twitter, DPC Watch Desk) for obtaining information that provides visibility of cyber threats and system vulnerabilities must be identified, documented and reviewed on a scheduled basis;
- Cyber threat and vulnerability information received must be assessed and prioritised to enable an appropriate response;
- Penetration testing of an external facing asset must be performed at least annually to detect cyber security vulnerabilities, with identified issues tracked and addressed in the *Corrective Actions Register*;
- Vulnerability remediation activities must follow change management processes and be applied in accordance with business requirements; Major patches must be adequately assessed and tested before deployed to the operational environment as per the *Project and Change Management Policy*.
- Unsupported Applications and Operating Systems should be replaced where possible; and
- Where non-supported systems / software must be used due to a business requirement, compensating controls must be applied. The presence of these systems / software must be recorded in the Legacy Software Register alongside the compensating controls that are implemented.

The *Risk Management Policy* must be followed to prioritise the implementation of identified mitigations or treatments. Identified security vulnerabilities in applications and operating systems must be patched or mitigated in accordance with the level of risk they pose to the company.

PATCHING OF APPLICATIONS AND OPERATING SYSTEMS

The patching of applications and operating systems is an essential and highly effective information security control. As part of threat and vulnerability management the following patching program must be in place for all PAE applications and operating systems:

- Patches, updates or vendor mitigations for security vulnerabilities affecting internet-facing services are applied within 48 hours if an exploit exists
- Patches, updates or vendor mitigations for less severe security vulnerabilities are applied within 2 weeks.
- Centralised Patching tools (e.g. Windows Server Update Service) should be used where possible to verify the application of patches and monitor patching compliance.

8. INCIDENT MANAGEMENT

The purpose of this section is to define PAE's requirements regarding identifying and responding to incidents and disruptive events with a primary objective to minimise the overall consequences experienced by the agency. Formalised cyber security incident response plans enable a consistent approach to the management of cyber security incidents.

PAE's incident management includes an Information Systems Incident Response Framework (ISIRF) to define the processes for planning for, responding to and recovering from cybersecurity incidents. The Information Security Incident Response Team (ISIRT) is responsible for implementing the ISIRF.

PAE's Information Security Incident Management Plan can be found Appendix E – **Information Security Incident Management and Appendix F – Specific Incident Response Procedures.**

ROLES AND RESPONSIBILITIES

All PAE employees and 3rd party contractors have a responsibility to report cyber security incidents.

The following key roles and responsibilities relating to PAE's incident management must be established and maintained.

Role	Responsibility
Director, Corporate Services	The Director, Corporate Services is responsible for overseeing the incident response and approving the decision as to whether to notify external parties.
Corporate Information Manager	The Corporate Information Manager is responsible for declaring an incident and informing the Director, Corporate Services The Corporate Information Manager will adopt the role of Team Lead. In his absence, the Team Leader, IT Operations will adopt this role.
Information Security Incident Response Team Leader	The Team Leader is responsible for ensuring that each incident is appropriately managed in alignment with the ISIRF.
Information Security Incident Response Team (ISIRT)	The ISIRT is responsible for carrying out the actions defined in the incident response plan. The ISIRT will be comprised of the following members: • Corporate Information Manager • Team Leader, IT Operations • Customer Experience Manager • Community Safety Manager • Governance Manager • Risk Manager

CYBER SECURITY INCIDENT RESPONSE MANAGEMENT

To effectively manage incident response, PAE must understand, develop and maintain capability to fulfil the following requirements:

- Obtain commitment of senior management;
- Develop, maintain and socialise the ISIRF;
- Establish the ISIRT;
- Obtain technical and other support (including operations support);
- Conduct information security incident response awareness briefings and training; and
Conduct information security incident response testing.
- Report incidents as required by regulation or law.

RESPONSE PLANNING

The ISIRT is responsible for developing, maintaining and testing response plans for high risk incidents (e.g. ransomware)

9. THIRD PARTY MANAGEMENT

The purpose of this section is to establish clear and consistent rules for governing third parties conducting business with PAE who have potential to impact PAE's information security (e.g. gain access to PAE information or systems).

This policy also defines the framework for managing access to PAE information by suppliers and their representatives.

THIRD PARTY SECURITY COMPLIANCE

All third parties engaging with PAE are expected to maintain a robust information security environment and protect the confidentiality, integrity, and availability of PAE information, and IT assets commensurate with the risks posed to those assets.

Suppliers are responsible for the safe custody of PAE information and IT assets when under their control.

THIRD PARTY SERVICES ASSESSMENT

When acquiring products and services PAE must preference suppliers and service providers that have demonstrated a commitment to secure-by-design practices and have a strong track record of transparency and maintaining the security of their own systems, services and cyber supply chains.

THIRD PARTY MATURITY ASSESSMENT

An assessment of the proposed or potential supplier must be performed prior to entering into a contract or agreement. The depth and breadth of this assessment is dependent on the classification of information associated with the service to be provided or the critical nature of the service. The assessment should consider:

- Existing certifications maintained by the third party, e.g., ISO 27001:2013;
- Attestation reports performed by independent auditors in line with reasonable assurance requirements;
- Performing a self-assessed (by the third party); or
- Engaging an independent auditor to perform a reasonable assurance audit on behalf of PAE.

SERVICE ASSESSMENTS

An assessment of the services to be provided by potential suppliers must be performed by the Corporate Information Manager or relevant manager prior to entering into a contract or agreement. This must consider:

- The classification of the information and/or IT assets involved in the service;
- The type and level of access to be granted to the supplier (logical and/or physical);
- The controls implemented and managed by PAE to manage the supplier's access to the information and/or IT assets;
- The resulting consequence levels involved with engaging a supplier to provide services to or on behalf of PAE; and
- The above details must be recorded in the Third Party Risk Register.

10. **SYSTEM ACQUISITION AND DEVELOPMENT**

PAE acquires and develops information systems to support its core business objectives. The intent of this policy is to ensure that security is given appropriate consideration when information systems are acquired and designed.

SYSTEM DESIGN AND PLANNING

The following must be observed with respect to system design and planning:

- Acquisition of new information assets must be authorised by the Corporate Information Manager;
- A security risk assessment of the acquisition must be conducted – which may be facilitated by the Corporate Information Manager or a delegate;
- Documented business requirements for new systems, or enhancements to existing systems, must specify the requirements for security controls, and be documented prior to the commencement of acquisition or development; and
- Design specifications must consider automated security controls to be incorporated into systems together with supplementary manual security controls necessary to support business requirements.

Newly Acquired Assets must be Identified and classified according to the requirements described in Appendix Asset Classification Standard

SOFTWARE DEVELOPMENT

Procedures for secure software development must be embedded into PAE's software development lifecycle. The following must be observed with respect to software development:

- Procedures for secure development, including testing and deployment, must be documented;
- Secure coding guidelines must be maintained for all programming languages used in software development;
- All personnel involved in software development must be trained on secure software development techniques;
- The software development lifecycle must abide by PAE's requirements defined in the *Project and Change Management Policy*;
- Security reviews, such as code audits, vulnerability assessments and penetration testing must be planned for and performed through all stages of the software development lifecycle;
- Test data must be protected and controlled such that it does not breach the classification which has been afforded to it in the production environment;
- Acceptance testing programs and related criteria must be established for new systems, or enhancements to existing systems;
- Procedures must be documented and implemented to prevent an individual performing unauthorised changes to the system; and
- Software development outsourced to a supplier must be supervised and monitored to ensure it meets the requirements of this policy.

Development Environment

- Access to the development environment and source code repositories must be restricted per the access requirements defined in the *User Authentication Policy*; and

- Development, testing and production environments must be separated to reduce the risk of unauthorised access or changes to production systems.

11. FACILITIES SECURITY

The purpose of this policy is to detail the physical security requirements for all PAE sites to ensure that assets are appropriately protected from physical and environmental threats.

SITE CATEGORISATION

PAE employs varying levels of physical security controls commensurate to the risks associated with the information and IT assets stored and accessed within these areas.

Levels of access for each PAE area must be identified and documented. Documentation must include:

The security zone of the area as per

- Appendix j - Security Zones; and
- Categories of employees who are authorised to access each area.

Classification of each zone must be made in accordance with a risk assessment and approved by the Corporate Information Manager.

FACILITIES SECURITY

The following requirements apply to all PAE facilities.

Employee Access

- Physical access must be granted on a need-to-access basis with authorisation from the appropriate manager, and revoked once no longer required;
- An audit trail of access in 'RESTRICTED' areas must be retained and reviewed periodically;
- Employees are adhere to the *End User Security Policy* with regard to physical security practices and incident reporting; and
- All employees accessing a PAE area must follow any site-specific access guidelines for that area.

Equipment Security

- Delivery of equipment or other goods into 'RESTRICTED' areas must be actively supervised and managed;
- Fixed infrastructure must not be taken off-site without prior authorisation from the Corporate Information Manager;
- Power and telecommunications cabling must be installed in accordance with relevant Australian Standards, as directed by the Australian Communications and Media Authority; and
- Building management systems must be in place in 'RESTRICTED' areas and configured to provide automatic alerts when relevant thresholds are exceeded (e.g. temperature, humidity, etc.)

Environmental Security

- Alternative power sources must be sufficient to cope with business requirements for continued system operation in the event of a loss of power;
- Cabling must be appropriately protected from accidental or deliberate damage or unauthorised access;
- Information assets vulnerable to environmental threats such as fire and flood must be appropriately protected from these threats;
- Computer systems must be appropriately protected from extreme temperature and moisture variations; and
- Environmental security equipment, including but not limited to air conditioners and fire safety equipment, must be maintained as per vendor recommendations to ensure its availability and integrity where required.

DOCUMENT CONTROL

ANNUAL EVALUATION AND REVIEW

This manual is subject to regular, ongoing management review by the CSWG and will be reviewed at least annually or when significant changes occur within PAE and the CSMS scope.

RELATED INFORMATION

This manual should be read in conjunction with the following supporting documentation:

- Cyber Security Governance Policy;
- The South Australian Cyber Security Framework; and
- The PAE Risk Management Framework.

OWNERSHIP AND APPROVAL

Responsible Officer	Corporate Information Manager
Approved By	Cyber Security Working Group
Last Reviewed	
Next Review Date	

VERSION HISTORY

Date	Version	Reviewed By	Summary of Changes
March 2022	0.1	Peter Kiley	Initial Draft
April 2022	0.2	Wayne Prideaux	Access review procedures
May 2022	0.3	Peter Kiley	Prepare for staff consultation

APPENDIX A - ASSET CLASSIFICATION STANDARD

The following standard is to be used for assigning a sensitivity classification to information assets. Over time, the classification of information may change due to a process or business requirement. For example, a Council strategy in its compilation stage may be classified as 'RESTRICTED', however once published to the community will become 'Public' or a Confidentiality Clause on a Council report is revoked.

There can also be an aggregated effect to data classification, for example:

- Information records such as archives will contain various records and are therefore likely to contain information with varying classifications;
- IT assets are likely to contain information of varying classifications; and
- Communications links can transmit data of varying classifications.

Data repositories and applications are to be managed according to the requirements of the highest classification of data held or transmitted.

CONFIDENTIALITY

Classification	Description
PUBLIC	Information authorised for unlimited public access and circulation. This includes information to be released due to a Freedom of Information request. Examples of information classified as 'Public' includes: • Media releases; • Marketing material following release; • Information on PAE's public websites; and • PAE strategies / annual report – post-release.
INTERNAL	Information is only available for official use by PAE employees and / or information that, by default, requires a Freedom of Information request or non-disclosure agreement or equivalent before it can be shared externally. Unauthorised disclosure, alteration or destruction of this information could have an adverse impact on organisational operations, assets, or individuals. Examples of 'Internal' information include: • Internal day-to-day correspondence (e.g. emails);

	• Commercially-sensitive business information; • Information on the intranet; and • Internal policies.
RESTRICTED	Information that is sensitive in nature and is restricted to authorised groups within PAE such as senior management or finance. Unauthorised release could reasonably be expected to cause harm to PAE or an individual. Examples of RESTRICTED information include: • HR and financial information; • Critical infrastructure and security assessment material (e.g. penetration testing reports); • Personally identifiable information ('PII') of community members; • Strategic planning information (pre-release); and • Confidential PAE reports.

INTEGRITY

Classification	Description
Low	'Low' requirement, such that there would be minimal impact if the data is inaccurate or incomplete.
Moderate	'Moderate' requirement, meaning that PAE would be somewhat affected by a loss of integrity, but the situation could be easily detected and recovered.
High	'High' requirement, meaning that a loss of integrity would cause significant disruption and embarrassment and might be difficult to detect.
Absolute	'Absolute' requirement, implying that no inaccuracies or omissions can be tolerated.

AVAILABILITY

Classification	Description
Low	'Low' requirement, meaning that loss of the data or service would have only a minor impact on PAE for an extended period (i.e., "best-effort" recovery).
Moderate	'Moderate' requirement, implying the loss would have a significant impact and recovery must be achieved within a period measured in days (typically 3 business days or less).
High	'High' requirement, meaning that loss would cause major disruption to PAE and recovery must be achieved within a period measured in hours (typically same business day).
Critical	'Critical' requirement, meaning that PAE would be crippled by the loss and recovery must be virtually instantaneous (no longer than a few minutes).

INFORMATION ASSET HANDLING GUIDELINES

Information must be labelled in a consistent manner to facilitate the identification of the information classification rating. It is also important the information is handled appropriately and as per its classification when it is distributed, transmitted, and stored, and disposed of securely.

Handling Type	PUBLIC	INTERNAL	RESTRICTED
Labelling	No labelling requirements.	No labelling requirements.	Label documents 'RESTRICTED' at the bottom of each page in capitals, bold and red as follows: 'RESTRICTED'
Distribution	May be freely disseminated to the public.	May be distributed freely within PAE and only to a third party if approved by the information owner.	Only distributed to authorised groups within PAE and only to a third party if a confidentiality agreement is in place.

Electronic Storage	Can be stored without restriction.	Must be stored on PAE-endorsed systems (e.g. not in personal cloud storage) only. Cannot be stored locally for an extended period of time (e.g. on laptop hard drive).	Must be stored on PAE systems only with access controls restricting access to authorised groups.
Electronic Transmission	Allowed without restriction.	May be transferred internally PAE without restriction.	Must be encrypted while in transit (e.g. LiquidFiles).
Electronic Media Destruction	Allowed without restriction.	Must be destroyed using PAE-approved methods.	Must use a specialist destruction service and obtain a destruction certificate.
Physical Transmission (e.g. USB transfer).	Allowed without restriction.	May be transported by hand by PAE staff only. Cannot be left in a public place for collection by the receiving party.	Must only be transferred in a sealed envelope using a secure courier. Portable media must be encrypted.

APPENDIX B - PAE PASSWORD STANDARD

Passwords / Passphrases are a critical component of information security. A sufficiently long and complex passphrase will be impractical to guess or reverse engineer and provides a high level of assurance for user or system accounts. A poorly constructed passphrase may result in the compromise of individual systems, data, or networks.

A strong pass phrase will consist of at least 14 characters ideally as 4 random words incorporating upper and lower case letters, numbers and symbols. Users should not use any of the following when creating a passphrase:

- Repeated characters (e.g. '1111');
- Arbitrarily mixed letters, numbers, or symbols (unless generating and storing the password within a password manager);
- Discoverable personal information (e.g. the user's birthday);
- Arbitrary numeric sequences (such as 1234567); or
- Previously used passwords.
- Song lyrics, movies, literature or word sequenced from any other publicly available material

Passphrases granting access to PAE information assets must meet the following standards:

Standard	Settings
Minimum passphrase length	14 characters
Passphrase expiry	If MFA in place for remote access to Virtual Desktops -> 365 days Otherwise 90 days.
Passphrase history	24 previous passphrases

APPENDIX C - PAE ACCOUNT NAMING STANDARD

Account names help to asset the identity of a user accessing a resource. Consistent naming greatly assist in the auditing and management of use accounts.

Standard	Settings
Network Account Name	<first name>dot<surname> Note: In the case of a name clash, append the next available digit starting from the number 1
Privileged Account Name	adm_<first name>dot<surname> Note: In the case of a name clash, append the next available digit starting from the number 1
Microsoft Azure Account	Microsoft Azure accounts will be the user's email address

APPENDIX D - SECURE LOGON STANDARDS

PAE information assets must be configured to meet the secure login standards:

- Accounts are locked after five (5) failed logon attempts;
- Locked accounts must not have a defined lockout duration and must be unlocked by an administrator before it can be accessed again;
- The passphrase entered is not displayed in clear text; and
- Systems are configured with a session or screen lock that activates after a maximum of 15 minutes of user inactivity or if manually activated by the user.

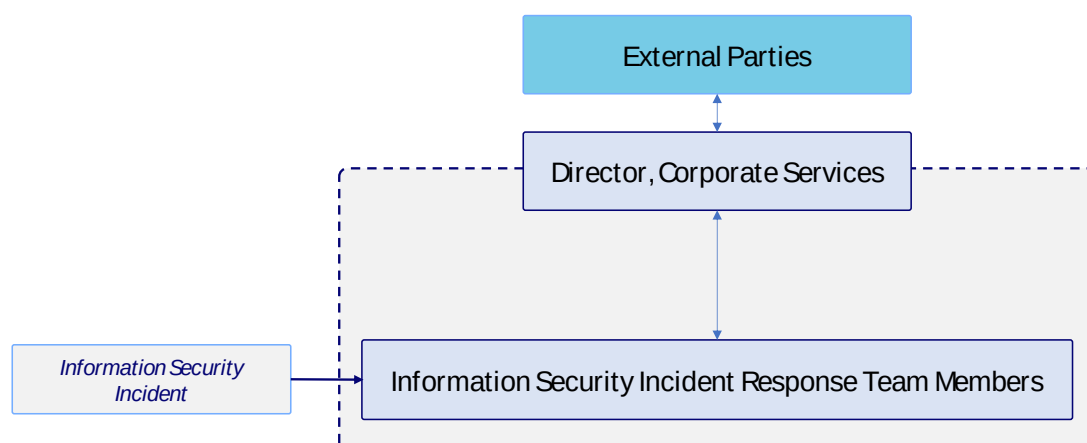
APPENDIX E - INFORMATION SECURITY INCIDENT MANAGEMENT

DEFINITIONS

Term	Definition
Information security <u>event</u>	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant.
Information security <u>incident</u>	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and/or threatening information security.

GOVERNANCE STRUCTURE

The following is a high-level overview of the information security incident response structure:



DIRECTOR, CORPORATE SERVICES

The Director, Corporate Services will be the primary point of contact between external parties and the ISIRT. External parties will be notified of the incident at the discretion of the Director, Corporate Services.

INFORMATION SECURITY INFORMATION INCIDENT RESPONSE TEAM

The Information Security Incident Response Team ('ISIRT') is charged with incident response management, and is comprised of the following individuals:

Incumbent	Individual	Backup Incumbent	Individual
Corporate Information Manager	Peter Kiley	Team Leader, IT ops	Wayne Prideaux
Team Leader, IT Operations	Wayne Prideaux	Network Administrator	Darren Alomes
Customer Experience Manager	Nikki Barnes	Customer Relations Officer	Stephanie Lee
Community Safety Manager	Brenton Thomass	Senior Community Safety Officer	Troy Martin
Strategy and Performance Manager	Lyn Guerin	Risk Manager	Daniel Dolatowski
Risk and Corporate Governance Team Leader	Daniel Dolatowski	Strategy and Performance Manager	Lyn Guerin

RESPONSE ACTIVITIES

Time	Activities
Pre-Event	Prior to an event, the ISIRT is required to: • Establish the member roles and responsibilities; • Ensure the ISIRF is maintained, and employees are accessible and contactable; • Design and participate in suitable incident response exercises; and • Ensure the ISIRT is adequately trained in incident response processes.
During an Event	During an event, the ISIRT is required to: • Collect information and assess potential information security events; and • Review potential information security events and declare an incident if required.
During an Incident	During an incident, the ISIRT is required to: • Determine and conduct the required response and recovery process; • Periodically communicate the status of the incident to the Director, Corporate Services; • Collate information for relevant authorities and individuals if required; and • Obtain support from external stakeholders (security specialist organisations, suppliers etc.) as required.

Post Incident	Following an incident, the ISIRT is required to: • Conduct a post incident review (PIR) and document any recommendations; • Review the ISIRT's performance and interaction with the Director, Corporate Services; • Debrief the Director, Corporate Services regarding the lessons learnt and recommendations; • Provide a report of the incident to authorities as required. • Obtain support from external stakeholders (e.g., forensics specialists) as required; and • Ensure this policy is updated as a result of any lessons learned, and the changes communicated to the ISIRT members.
---------------	---

COMMUNICATION

The ISIRT Team Leader will coordinate communication efforts internally.

The Director, Corporate Services will coordinate external communication efforts groups such as:

- Community;
- Media;
- State government;
- Employees;
- Vendors; and/or
- Other authorities.

INTERNAL COMMUNICATION OF INFORMATION SECURITY EVENTS

Identified information security events shall be reported initially to the Corporate Information Manager, who may declare an information security incident.

INTERNAL COMMUNICATION DURING AN INFORMATION SECURITY EVENT

If an incident is declared, communication from the ISIRT to the Director, Corporate Services and relevant internal parties is critical for the successful management of the incident and the ongoing response process.

EXTERNAL COMMUNICATION

Within the context of the ISIRF, external communication is considered any communication outside of PAE. During an information security incident, the following external communication requirements shall be met:

- As soon as the cause and possible extent of the incident is determined, and depending on the event/cause, the Director, Corporate Services will draft statements for release.
- ISIRT members must work with the Director, Corporate Services to develop any statements.

- Communication made by the Director, Corporate Services or authorised personnel at the time of any information security incident will supersede the information contained in this document.

INCIDENT RESPONSE FRAMEWORK ('ISIRF')

The information security incident response process follows a set number of phases. While each incident will be unique, these phases provide a way to logically and methodically manage any incident. These phases are:

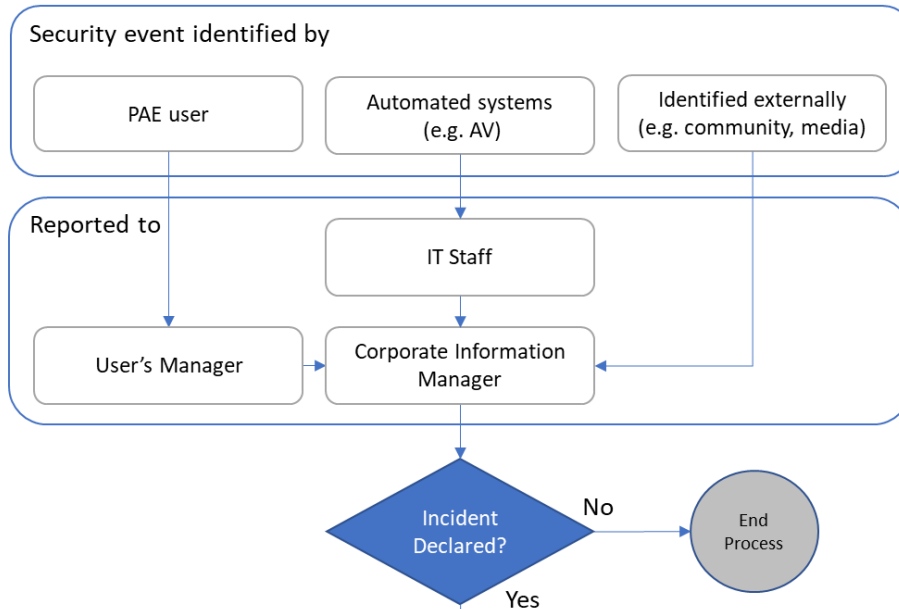
1. Planning and Preparation
2. Identification
3. Containment & Eradication
4. Recovery
5. Post-Incident Review

PROCESS OVERVIEW

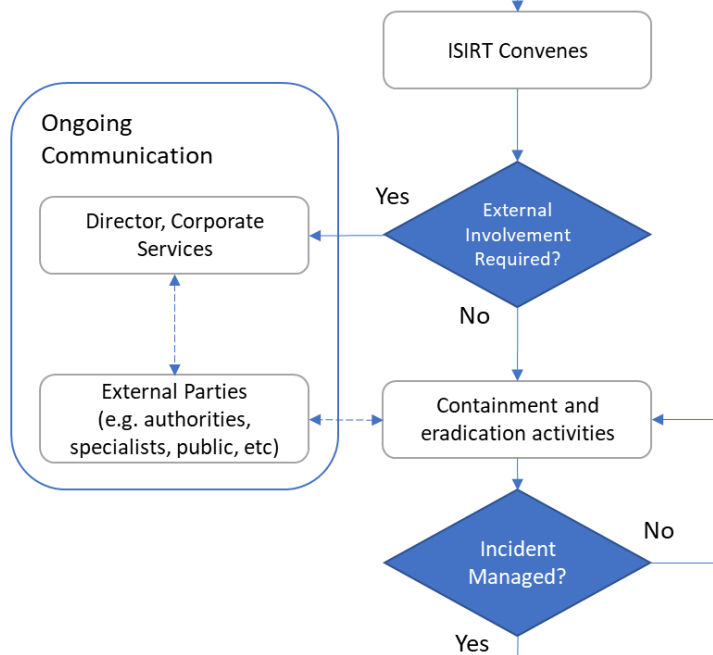
1. Planning & Preparation

Ongoing Incident Response
Training and Testing

2. Identification



3. Containment & Eradication



4. Post Incident Review



1. Planning and Preparation Phase

It is critical that PAE's capability to respond is maintained and tested before an incident occurs. All personnel must be made aware of their responsibilities and provided with appropriate training. In particular, members of the ISIRT and other staff holding key incident management roles should be familiar with the latest process and procedures. Periodic testing is an effective way to assess PAE's readiness to respond to an incident.

2. Identification

Information security events must be reported to the Corporate Information Manager. Events may be identified from a variety of internal and external sources, including but not limited to:

- PAE's employees and members;
- PAE's automated systems;
- Community;
- The media;
- Other councils;
- State government organisations; and
- Service providers or other external organisations.

Refer to *Appendix M - Sources of Precursors and Indicators* for further information to support the detection of events.

While it is ideal for the IT team to gather and record as much information as possible regarding the event, it is more important to report a potential information security incident in a timely manner rather than to be complete with all information. The minimum information to collect includes:

- When did the reporter detect the event(s)?;
- What are the reporter's observations?; and
- What are the Corporate Information Manager's observations?

Assessment and Reporting

Once an information security incident is declared by the Corporate Information Manager, it will be escalated to the Director, Corporate Services who will then determine who shall be notified of the incident (e.g. Board, authorities, etc).

The Director, Corporate Services and Corporate Information Manager will then agree whether specialist third party assistance is required.

3. Containment and Eradication

The primary goal during this phase is to mitigate the impact of the threat and restore service / protect information as necessary. The secondary goal is to establish the root cause.

The following will be performed once an incident is identified:

- The ISIRT is convened to manage the incident;
- The ISIRT performs steps to protect information and restore services in response to the incident. This may include actions such as taking the affected systems offline and restoring them to supporting infrastructure where possible; and
- The ISIRT provides the Director, Corporate Services with periodic updates regarding the incident status.

4. Post Incident Review

Once the incident is under control, further review should be performed by the ISIRT to determine the root cause. Third party forensic specialists may be engaged to support these activities.

Once the incident is over it is important to immediately determine the following:

- Does PAE have any ongoing responsibilities to affected parties?
- Do any of the ISIRT team members need extra support?

Following this, it is important to capture any learnings from the incident. This includes:

- Why did the incident occur?
- Is it reasonable that the incident occurred?
- What did and did not work well in the incident response?
- What improvements can be made?
- Does any PAE documentation require updating?

PAE should also ensure that any further information security vulnerabilities detected during the incident are addressed.

LESSONS LEARNED

The post-incident review requires PAE to reflect on how the incident occurred and how well the incident was managed. The exercise should include the following activities:

- Ascertain whether similar incidents have occurred before.
- Assess whether the incident was correctly categorised and prioritised.
- Analyse the root cause.
- Determine whether the ISIRF or supporting response plans require amendment.
- Review the corrective actions to identify whether, in hindsight, the most effective course of action was taken.

With due care of confidentiality aspects, information security incidents should be used in user awareness training as examples of what could happen, how to respond to such incidents and how to avoid them in the future.

Information collected during the investigation of an incident should be used to identify recurring or high impact incidents. This information may indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences.

Recurring incidents should be identified and reported to the Director, Corporate Services for further risk assessment. The Director, Corporate Services is responsible for providing resources to prevent similar incidents from reoccurring.

POST INCIDENT REPORTING

A post-incident report (PIR) should be presented to the Director, Corporate Services once the incident has been closed. The report should:

- Provide an overview of the incident.
- Highlight the root cause of the incident.
- Provide detailed commentary on what went well or not so well in the investigation / recovery / eradication of the issue.
- Recommend improvements and provide associated costs (where possible).
- Document any risk in not taking the recommended actions.

Any actions arising from the PIR should be recorded within the Corrective Actions Register within PAE. The completed PIR must be retained as a corporate record for future reference and be signed off by the Director, Corporate Services.

APPENDIX F - SPECIFIC INCIDENT RESPONSE PROCEDURES

Steps To Take During a Ransomware Attack

Initiate Incident Response Team	
Action	Responsibility
We will need to act quickly, but methodically. Stay calm, and enact the planned incident response (IR) steps defined in Appendix E.	Corporate Information Manager or Team Leader IT Operations
Brief the Incident Response Team on the potential impact the security incident may cause. Take into consideration not only those areas that are obviously compromised, such as data being encrypted and applications being down, but also additional areas of potential compromise.	Corporate Information Manager and Team Leader IT Operations
Inform the Media, Marketing and Communications Team so they can begin to prepare. Let them know you will establish a more formal communications and reporting structure as you gather additional information	Incident Response Team
Establish a communications and update protocol with a designated contact for each business unit. For example, commit to updating all relevant team leads every three hours on the situation. This is an important step to avoid people constantly asking for updates and preventing the IT team from focusing on containment.	Incident Response Team

Isolate Your Systems and Stop the Spread	
Action	Responsibility
Assess options for isolating the threat to stop it from spreading. If the incident is already known to be widespread, decide if we should implement blocks at the network level, such as isolating traffic at the switch or the firewall edge, or temporarily take down the internet connection. If the incident scope is already confirmed to be more narrow, infecting only a few systems, you could isolate them at the device level by possibly pulling the Ethernet or disconnecting the Wi-Fi	Corporate Information Manager and Team Leader IT Operations and Network Administrator

Remember to try and keep all systems powered on to ensure no forensic evidence is lost. And keep in mind that once you disrupt an attacker's activity, you are tipping them off and they may go dormant, making it harder to identify the entire attack scope.	Team Leader IT Operations and Network Administrator
--	---

Identify the Ransomware Variant	
Action	Responsibility
Many of the tactics, techniques, and procedures of an attack are publicly documented for each ransomware variant. Determine which attack we are dealing with to obtain information on where to look for the threat and how it is spreading, as well as details around persistence	Team Leader IT Operations and Network Administrator
Depending on the variant, some decryption tools may already be available to decrypt our ransomed files. Check the No More Ransom website. Oftentimes, the ransom note itself will give us a good indication of the ransomware group and/or variant being used. Uploading the ransomware to ID Ransomware may help identify the variant.	Team Leader IT Operations and Network Administrator

Identify Initial Access	
Action	Responsibility
Determining the initial access point, or patient zero, will help us close the hole in your security. Common initial access vectors are phishing, exploits on your edge services (such as Remote Desktop services), and the unauthorised use of credentials. Other initial access vectors could be drive-by compromises, exploits on public-facing websites and applications, removable media, hardware additions, and supply chain compromises.	Team Leader IT Operations and Network Administrator
This step is sometimes difficult, and we may need expertise from digital forensics or IR experts and consultants in determining the initial point of access. Based on advice from the previous activity; decide if external assistance is required and commence engagement activities. Possible Suppliers: Cyber CX Sarah Taylor Account Manager SA m: 0407 277 183 e: sarah.taylor@cybercx.com.au www.cybercx.com.au Level 2, 136 Greenhill Road, Unley, SA 5061	Corporate Information Manager

locane Mike Vasileff Account Manager M: 0414 730 387 P: 1300 462 263(1300 IOCANE) A: 763 South Road, Black Forest SA 5035 E: mike.vasileff@iocane.com.au	
Depending on the variant, some decryption tools may already be available to decrypt your ransomed files. Check the No More Ransom website. Oftentimes, the ransom note itself will give a good indication of the ransomware group and/or variant being used. To help identify the variant uploading the ransomware to ID Ransomware.	Team Leader IT Operations and Network Administrator

Identify All Infected Systems and Accounts (Scope)	
Action	Responsibility
Even after an attack is over, it is possible that attackers still have a foothold in our network. Identify any active malware, or persistent leftovers that are still communicating back to the attacker. Persistence techniques include: Creating new processes running the malicious payload Using run registry keys Creating new scheduled tasks. Check for signs on all servers.	Team Leader IT Operations and Network Administrator
The attackers have most likely compromised a number of accounts, both non-privileged and privileged, such as Active Directory (AD) accounts, so disable any suspect accounts.	Team Leader IT Operations
Ensure there are no new rogue account creations in process	Team Leader IT Operations
Review other AD components, such as Group Policy Objects (GPOs), to determine if anything has been newly created or modified. This is a common tactic used by attackers to push the ransomware payload out to all systems	Team Leader IT Operations
Document the findings <u>before taking action</u>. Taking action may alert the attacker and cause them to launch a much more serious attack. It may also limit your ability to recover your data or determine the full impact of the data breach	Team Leader IT Operations

Determine if Data Was Exfiltrated	
Action	Responsibility
Often times, ransomware attacks not only encrypt our files but they also exfiltrate our data. They will do this to increase the chances that we will pay the ransom by threatening to post things like proprietary or embarrassing data online. Check the firewall for signs of data exfiltration, such as large data transfers, on our firewall devices. n This step can also be difficult and may be another situation to consider bringing in a digital forensics team or IR expert consultants for a more thorough investigation.	Team Leader IT Operations and Network Administrator
Decide if external assistance is required and commence engagement activities	Corporate Information Manager

Locate Your Backups and Determine Availability	
Action	Responsibility
A ransomware attack will attempt to wipe our online backups and shadow copies to decrease the chances of us recovering our data and ultimately not paying the ransom. Check our backups have not been affected by the incident and is still operational. Verify if our online and offline backups are available for recovery.	Team Leader IT Operations and Network Administrator
Engage with offsite backup provider if necessary. Contact details. Maurice Hewson State Manager SA/NT TIMG Australia T 08 8416 5606 M 0419 605 369 F 1300 669 140 timg.com	Team Leader IT Operations

Verify the Integrity of Your Backups and Restore To Last Known Good	
Action	Responsibility

With many ransomware attacks, attackers have usually been in the network for days, if not weeks, before deciding to encrypt your files. This means that we may have backups that contain malicious payloads that we do not want to restore to a clean system. Through investigation of the incident, we should gain a good idea of the initial access date and time. Try to restore from the day before after scan the backups to determine their integrity.	Team Leader IT Operations and Network Administrator
---	--

Sanitize Systems or Create New Builds	
Action	Responsibility
Based on our ability to identify all of the active malware and incidents of persistence in our systems, make a recommendation to the Incident Response Team on the recovery action; eg database restores, file system restores, clean builds etc. Take into account time savings by not rebuilding. However, it may just be easier and safer to create new, clean systems. Consider building a totally separate, clean environment that we can then migrate to. Make sure when we rebuild or sanitize the network or network segment, you have security controls installed and are following best practices to ensure devices do not become reinfected.	Corporate Information Manager and Team Leader IT Operations and Network Administrator
Review the recommendation and decide recovery method.	Incident Response Team

Report the Incident	
Action	Responsibility
Consider the reporting requirements and needs; Local Government Risk Services Report Cyber (https://www.cyber.gov.au/acsc/report) Seek any legal advice to help address any legal obligations around regulated data, such as PCI.	Corporate Information Manager and Finance Manager and Risk & Corporate Governance Team Leader
Determine if we will publicly disclose the attack. In some cases, we may be legally required to disclose some or all details around the network. Determine the time frame within which we must disclose the attack, if required.	Incident Response Team

Paying the ransom	
Action	Responsibility
It is not recommended that the ransom be paid. However, if paying the ransom is a consideration, we should hire a resource/company with specialised skills to help us negotiate the ransom down. The bad actors are usually willing to negotiate. We should only negotiate to get our data back. Also remember that there is never a guarantee that negotiating with the attacker will stop them from deleting data or releasing our data publicly. When negotiating, if the attackers claim they have stolen our data, ask them to provide a verifiable sample of the stolen data, such as a directory structure. They will typically provide that proof. Keep in mind that paying the ransom is not going to remediate the vulnerabilities that the attackers exploited, so still ensure we have identified the initial access and patched the vulnerabilities.	Incident Response Team

Conduct a Post-incident Review	
Action	Responsibility
Review our incident response to understand what went right and to document opportunities for improvement. This “lessons learned” step helps ensure the continuous improvement of our response and recovery capabilities. It is worth noting that this review should be done as soon as possible after the recovery phase, while it’s all fresh in everyone’s mind.	Incident Response Team

APPENDIX G - ICT STANDARD OPERATING PROCEDURES

ACCESS ADMINISTRATION PROCEDURES

ACCESS MANAGEMENT

User Access provisioning procedure

Users are to be provisioned in accordance with standards specified in Section 5 of the Cyber Security Manual.

The following procedures apply;

Receive Request and verify its validity	
Action	Responsibility
Requests for user access or change are typically received via an ECM task initiated by the P&C Team or a Fresh Service request for contractors or access extensions. Every request outside of the ECM tasks is to be recorded as a ticket in Fresh Service. Assess the request and if there is any doubt about its validity or appropriateness for the role being performed, confirm with the Information Asset Owner or the staff member's Manager. Record the action taken as a note on the ECM task or fresh ticket.	IT Operations team member.

Action the request	
Action	Responsibility
For new users; Complete the request in accordance with the instructions specified in Appendix N – Work Instruction enrolling user.	IT Operations team member.
For existing users with changes; Complete the changes (eg access to alternate roles in Technology One) and check each other access type is still correct.	IT Operations team member.
Complete the check list to nominate actions taken as per Appendix N – Work Instruction enrolling	IT Operations team member

user. Paste as note in Fresh or against the ECM Task.	
---	--

Quality Control	
Action	Responsibility
Request another team member review the check list and confirm that the user changes have been completed in accordance with the request.	IT Operations team member.
Add a note to Fresh or ECM with the results of the review.	IT Operations team member.(reviewer).
Close out any issues found.	IT Operations team member

Finalise new user	
Action	Responsibility
Upon completion of the user set up ensure the user's password is set to 'Change at next login'	IT Operations team member.
<i>The user is required to attend the IT section and login for the first time on a computer in the IT area. The password is provided at login time or entered by IT staff.</i> <i>If the user is an 0365 user, they will login to Azure and setup Multi Factor Authentication.</i>	IT Operations team member.
Provide the user with access to "Intro to common Apps"	IT Operations team member

Privileged User Access provisioning procedure

Privileged users are to be provisioned in accordance with policies specified in Section 5 of the Cyber Security Manual.

The following procedures apply;

Receive Request and verify its validity	
Action	Responsibility

Requests for privileged user access or change are to be recorded as a Fresh Service request. Treat the request as a 'change request' and action in accordance with Appendix H – Change Management. If the staff member/contractor is not a member of the Corporate Information Section, add an entry to the Cyber Security Exceptions register. Record the action taken as a note on the fresh ticket.	IT Operations team member.
--	----------------------------

Action the request	
Action	Responsibility
For new users; Privileged users will have two accounts; a standard account with no admin privileges and a privileged account with limited access to email and internet. Complete the request in accordance with the instructions specified in Appendix N – Work Instruction enrolling user.	IT Operations team member.

User Access Removal Procedure

Process for removing standard and privileged accounts inline with policy. Consideration around shared account credential handling on employee exit.

Leaders are required to fill out a staff separation form for ALL employees, agency staff and work experience students who will be leaving PAE, or who are taking long term leave.

Any devices assigned to the leaving staff member will need to be returned to IT to be reallocated. Any keys or FOBs are to be returned to Property Services

The following procedures apply;

Manage separation requests	
Action	Responsibility
Requests for staff separation are received via staff separation form. When staff are known to have left but no separation form has been received; followup with staff members leader.	IT Operations team member.

If no separation form has been received within 30 days of a known separation; the Team Leader IT Operations can authorise removal.	Team Leader - IT Operations
Where staff members are on long term leave or a long term absence and the account is not removed; add this as an entry in the cyber security exemption register.	Team Leader - IT Operations

Action the request	
Action	Responsibility
Remove domain access	IT Operations team member.
Make the H Drive a shared folder and place in the Departments G Drive with the name Old_<username>_HDrive.	IT Operations team member.
Remove user from AD Groups.	IT Operations team member
Add user to Shared_Mailbox group. Add the expiry date as description in AD	IT Operations team member
Remove the users licenses from O365	IT Operations team member
Technology One – Set User Status to “Not a User of this Product” and Disable Account	IT Operations team member
Fresh Deactivate User Account	IT Operations team member
Known common accounts (eg Library front counter) – To be determined.	IT Operations team member
Exchange – restrict use (remove so not in global address book) – make a shared account. Set Message delivery restriction add Admin as selected sender to receive messages from.	IT Operations team member

Quality Control	
Action	Responsibility
Request another team member review the check list and confirm that the user separation has been completed correctly.	IT Operations team member

Close out any issues found.	IT Operations team member
Register the completed request (QAP 157 – HR Staff Separation) and checklist in ECM.	IT Operations team member.

User Access Review Procedure

User access reviews will occur periodically. Work instructions and frequency are defined in Appendix O – Work Instructions Access Review.

Review of IT area perimeters (Computer and Comms facilities) procedure

IT has a range of areas or interest that may contain switches/routers, patching panels, UPS (uninterruptible power supplies), Wireless Access Points or even Servers and SANs (Storage area Networks) or even Fibre Paths.

In general Servers and SANS are secured in their respective Server / Computer Rooms located at either the Civic Centre or Port Adelaide Library.

Smaller sites may have a Comms Room or a simple rack for their patching and switches/routers.

Securing of the larger purpose-built areas has more often included a BMS Managed electronic access control, whereas the small sites have been simple keyed solutions.

The purpose of this section of the document is to set guidelines and procedures in place and encourage IT Staff to develop a practice of using any site visit or walk past as an opportunity to check security of the IT Areas and where possible resolve any compromised areas.

The frequency of the (IT) perimeter review will be as per the Cyber Security Calendar.

The following procedures apply;

Daily Check	
Action	Responsibility
After Close of Business of each working day IT Staff rostered to perform “End of Day” to perform security check of Civic Centre IT Areas including doors secure and free handle not enabled. <tag the door>	IT Operations team member.

ADHoc Site Visit Check	
Action	Responsibility
IT Staff performing site visit to perform security check of sites IT Areas and where applicable including doors secure and free handle not enabled	IT Operations team member.

Prepare for review – IT Areas Perimeters	
Action	Responsibility
Confirm the list of sites to be reviewed with the Team Leader IT Operation. Refer; ECM Subject Ref - “External Access to Council's Computer System” Document Common Number 15940908 Title - Location of list IT Areas Perimeter Review - Access Control to Physical Areas – Save Document as Access Control to Physical Areas – Month YYYY and register in ECM under same Subject as Template document.	IT Operations team member.
Create Fresh ticket for the review	IT Operations team member
Any agreed changes to the scope of the review to be noted with the Fresh Ticket	IT Operations team member
Undertake review	
Action	Responsibility
Undertake the review; record results in inspection template – Confirm the list of sites to be reviewed with the Team Leader IT Operation. Update relevant period review document using Checkout and Save and Version in ECM.	IT Operations team member.
Complete any follow up actions from the review	Team Leader - IT Operations
Complete review	
Action	Responsibility
Record all notes against Fresh Ticket; attach a copy of the inspection results and ensure completed period review document is registered in ECM	IT Operations team member.

Prepare for review - BMS Access Granted (Schneider System)	
Action	Responsibility
Monthly run Reporting Services Report INET004_1 IT Doors Access	Team Leader - IT Operations

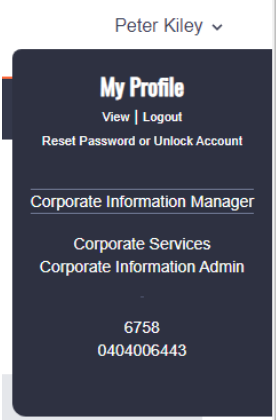
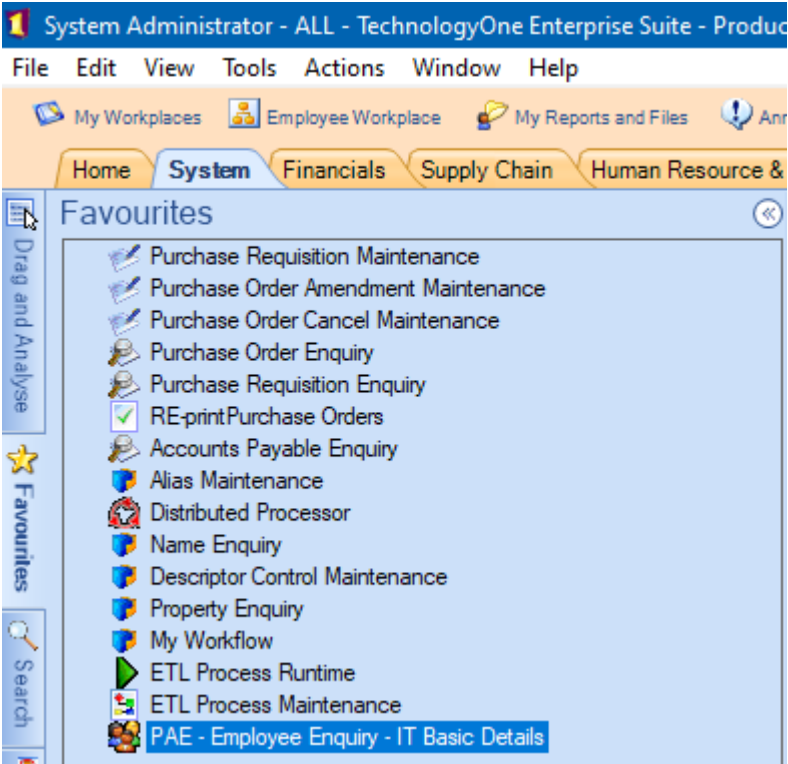
Undertake review	
Action	Responsibility
Undertake the review; markup names requiring investigation on report with recommended action and register and Task in ECM to Property & Building Team	Team Leader - IT Operations
Property & Building Team member to perform any actions from the review	Property & Building Team
Complete review	
Action	Responsibility
Record all notes of action taken against ECM document	Property & Building Team

Password Reset/Account Unlock Procedures

For standard users (non Privileged accounts) there are two types of users; Domain/Active Directory (AD) Users and Technology One (T1) only users and two types of requests; Password change and Account Unlock.

The procedures are effectively the same with exceptions noted below;

Access Requests	
Action	Responsibility
For walk up/phone requests - determine the type of reset to be performed. For AD Users confirm they have access to AD Self Service from the Intranet and request they self serve if possible.	IT Operations team member

	
If the request is for a changed password, when the staff member is not recognised; look up their details in Technology One using the “PAE- Employee Enquiry – Basic IT details” function and ask them to confirm at least two details (eg home address and birthdate). Do not continue until this has been completed satisfactorily. 	IT Operations team member
For users with privileged accounts; • identification is to be done in person.(ie no password resets are to be done over the phone) • password changes will include the requirement to change at next login	IT Operation Team Member
Use a passphrase generator to create password to privileges accounts.	Privileged Account Holders

Any exception to this process for privileges accounts will be subject to Corporate Information Manager approval and be recorded in the Cyber Security exceptions register.	IT Operation Team Member
--	--------------------------

Action Request	
Action	Responsibility
For account unlock requests; Unlock the account.	IT Operations team member
For password reset requests, change the password to a unique passphrase and set the users account to require a password change at the next login.	IT Operations team member
Create a Fresh Ticket to capture the password change request.	IT Operations team member
Report to the CSWG on a regular basis (typically quarterly) on the number of password resets performed.	Corporate Information Manager

SYSTEM PROVISIONING

Workstations

Include processes specifically required for hardening (Macros, Flash/Java, block admin actions) and aligned to CSM hardening Policy.

Servers

Include processes specifically required for hardening (Macros, Flash/Java, block admin actions) and aligned to CSM hardening Policy.

Mobile Devices

Include process to authorise personal mobile phones to access PAE emails.

VULNERABILITY MANAGEMENT

System Patching Procedure(s)

This SOP would be considered a primary cyber security function

Patching Compliance Procedure

Process to confirm alignment to expected patching compliance rates. Initially Windows systems (via WSUS) but also look to leverage Intune for reporting. Extend to other systems over time (network devices, Applications). This may require a vulnerability management system)

APPENDIX H - PROJECT AND CHANGE MANAGEMENT GUIDELINES

PAE engages in project delivery and change management to support its core business objectives. This policy is designed to govern when and how to apply requirements for addressing risk within projects and changes affecting PAE information and IT assets.

PROJECT AND CHANGE TYPES

PAE categorises projects and changes into the following:

Type	Description	Examples
Incidental or Minor	Very low risk. Most changes will fall into this category. Impacts a single user or small team.	Regular patching of operating systems Installation of an application for an individual
Moderate	A change that presents a moderate risk to PAE. Some changes and most projects will fall into this category. Impacts more than one team using a system that has restricted confidentiality, high integrity or high availability.	Installation of a patch on a mission critical application
Major	A project or change that will affect a large number of users or has the potential to cause significant harm or interruption of services.	Server installation Version update of a mission critical application Moving data centre Deployment of a new application

PROJECT AND CHANGE MANAGEMENT REQUIREMENTS

PAE requires that projects and changes be managed proportionally to the risk that they present to the organisation. The following requirements apply:

Type	Approval	Examples	Communication	Recording	Backout Plan
Incidental or Minor	Pre-approved	Brief test plan	Not required	Not required	Not required
Moderate	Corporate Information Manager	Pre and post implementation testing	Email to affected users	Recorded in change register	Not required
Major	Director, Corporate Services	Formal test plan	Formal communications plan	Recorded in change register	Required

MAJOR PROJECTS AND CHANGES

Major changes present a significant risk to PAE. As such, rigorous controls are in place to ensure that the risk is appropriately managed. The procedure for a major change is as follows:

1. A need is identified and documented;
2. A project or change request is raised in the IT Service Management tool (Fresh);
3. All affected parties and systems are identified and documented;
4. A risk assessment of the change is performed and documented;
5. A risk treatment plan is developed;
6. A communications plan is developed;
7. A test plan is developed;
8. The change request is submitted to the relevant Director / information owner for review and approval;
9. The communications plan is enacted;
10. Pre-deployment testing is performed;
11. The change is implemented;
12. Post-implementation testing is performed;
13. Testing results are recorded and submitted to the Corporate Information Manager for closure approval; and
14. The change is closed in the IT Service Management tool.

Testing and communication strategies for these changes will be unique to the change. As a baseline, all major changes to publicly facing systems must undergo independent penetration testing.

Similarly, full back up and restoration processes must be tested when major IT infrastructure changes occur to validate procedures and ensure defined recovery timeframes can be met.

Vulnerability Assessments and Penetration testing activities must be considered during the implementation of a new system or when projects is undertaking significant changes to a system.

MODERATE PROJECTS AND CHANGES

Moderate projects and changes do not present a significant risk to PAE. For this reason, less testing and authorisation is required prior to implementation. The procedure for a moderate change is as follows:

1. A need is identified and documented;
2. A change request is raised in the IT Service Management tool;
3. All affected parties and systems are identified and documented;
4. A brief test plan is developed;
5. The change request is submitted to the Corporate Information Manager for review and approval;
6. All affected parties are notified;
7. The change is implemented;
8. Post-implementation testing is performed;
9. Troubleshoot issues if required; and
10. The change is closed in the IT Service Management tool.

INCIDENTAL OR MINOR CHANGES

Incidental or minor changes are low risk changes that occur as part of business-as-usual activities. Incidental or minor changes do not need to comply with formal change management processes.

EMERGENCY CHANGES

At times it may be necessary to fast track a change in response to a serious issue. In such situations it may not be practical to complete the standard change process. Approval to implement an emergency change must be obtained from the system owner before commencement. After the change is complete the relevant change process must be completed retrospectively.

APPENDIX I - BACKUP AND DATA PRESERVATION

DAILY BACKUP CHECKS

This is a key cybersecurity procedure which should be documented. Priority on key systems / data.

SYSTEM RECOVERY PROCEDURES

Should include at least systems with 'High' availability requirements

SYSTEM RECOVERY PROCEDURES

Specific procedures to enable testing of recovery procedures. May be incorporated into the baseline recovery procedure.

APPENDIX J - SECURITY ZONES

The following table describes the PAE security zone model.

It should be noted that a site may contain higher-zone areas within its perimeter.

Security Zone	Site Description
PUBLIC	Uncontrolled sites where the general public may be present. Such areas include: • Libraries; • Council office foyers and front desks; • Home offices. Note: 'Public' sites with public operating hours shall be considered 'Internal' outside of those hours.
INTERNAL	Controlled sites accessible by PAE personnel and limited public/visitors. Such areas include: • Building perimeters; • Shared meeting room and interview areas; and • Offices and coworking spaces shared with other tenants.
RESTRICTED	Sites where physical security controls are entirely managed by PAE. Access is limited to certain PAE employees and authorised personnel. Public access is not permitted. Such areas include: • Server rooms; and • Secure comms rooms.

Control Area	PUBLIC	INTERNAL	RESTRICTED
Physical Access Controls	Access to the site is uncontrolled.	Access to the facility must be limited by an access card or key issued by PAE. A register of access cards or keys must be kept.	Access to the facility must be limited by a PAE identity access card to select individuals.
Perimeter Controls	Access to the site is uncontrolled.	All doors used to access the facility must be controlled by an electronic access control system. All perimeter doors must be covered by CCTV.	This zone must be layered inside an 'Internal' zone. All doors used to access the zone must be controlled by an electronic access control system which is logged.
Alarm System	Access to the site is uncontrolled.	A monitored alarm system must be deployed. Alarm system operators and users must be appropriately trained and approved for access to the area.	An alarm system must be deployed. Control of the alarm system must be directly managed by PAE.
Visitors/Contractors	Visitors must sign into Sine and be advised of the facility security requirements they must adhere to.	Visitors must be escorted at all times. Visitors must sign into Sine and be advised of the facility security requirements they must adhere to.	Visitor access is granted on a strictly need-to-know basis with management authorisation. Visitors must be closely escorted at all times.

APPENDIX K - SOFTWARE DEVELOPMENT

SECURE DEVELOPMENT, TESTING AND DEPLOYMENT

PAE acquires and develops information systems to support its core business objectives. The intent of this manual is to ensure that security is given appropriate consideration when information systems are acquired and designed.

SYSTEM DESIGN AND PLANNING

The following must be observed with respect to system design and planning:

- Acquisition of new information assets must be authorised by the Corporate Information Manager;
- A security risk assessment of the acquisition must be conducted – which may be facilitated by the Corporate Information Manager or a delegate;
- Documented business requirements for new systems, or enhancements to existing systems, must specify the requirements for security controls, and be documented prior to the commencement of acquisition or development; and
- Design specifications must consider automated security controls to be incorporated into systems together with supplementary manual security controls necessary to support business requirements.

SOFTWARE DEVELOPMENT

The following must be observed with respect to software development:

- Procedures for secure development, including testing and deployment, must be documented;
- Secure coding guidelines must be maintained for all programming languages used in software development;
- All personnel involved in software development must be trained on secure software development techniques;
- The software development lifecycle must abide by PAE's requirements defined in the *Project and Change Management Policy*;
- Security reviews, such as code audits, vulnerability assessments and penetration testing must be planned for and performed through all stages of the software development lifecycle;
- Test data must be protected and controlled such that it does not breach the classification which has been afforded to it in the production environment;
- Acceptance testing programs and related criteria must be established for new systems, or enhancements to existing systems;
- Procedures must be documented and implemented to prevent an individual performing unauthorised changes to the system; and
- Software development outsourced to a supplier must be supervised and monitored to ensure it meets the requirements of this policy.

Development Environment

- Access to the development environment and source code repositories must be restricted per the access requirements defined in the *User Authentication Policy*; and

Development, testing and production environments must be separated to reduce the risk of unauthorised access or changes to production systems

SECURE CODING STANDARDS

All web applications which are exposed to the public would have the following standards as a minimum:

1. All communications with outward facing web apps must be done securely using SSL (https) – this prevents attackers from listening in to traffic and prevents man-in-the-middle attacks.
2. Password management – use of Multi-Factor Authentication for users is preferred, especially when accessing sensitive data. At a minimum, there will be password restrictions such as minimum length, use of more complex numbers / symbols, passwords must be changed regularly.
3. User passwords must be hashed with a user “salt” and a secure hashing function must be used. Examples of secure hash functions that should be used: ¹
 - a. bcrypt
 - b. scrypt
 - c. PBKDF2 (using SHA-256)
4. Access to api endpoints and pages must be secured and restricted (especially to non-public data and endpoints which modify data); this includes both a check to make sure the request came from a logged in user and that the user has enough rights to perform the requested action.
5. SQL injection must be prevented by:
 - a. Sanitising & validating user input
 - b. Using SQL parameters instead of building up raw SQL query within a string
6. Prevent Cross Site Scripting (XSS) attacks by: ²
 - a. Not using user-entered data directly where possible
 - b. Where this is not possible,
 - i. User entered data is encoded before being used in the DOM, and /or
 - ii. User entered data must be sanitised and any HTML tags, etc are stripped before being saved in the database
7. Cookies must be secure (especially cookies which store user data or a cookie to determine if a user is logged in). Cookies must either be encrypted or have the HttpOnly flag set to prevent them from being accessed by JS. Login cookies must be validated against known and valid cookies in the database with an expiry date to prevent forgery and replay attacks with cookies.

¹ this list will be updated as best-practises for hashing functions change

² more details can be found here:

https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

APPENDIX L - PROCUREMENT PROCEDURES

CONTRACT SPECIFICATION GUIDELINES.

Third party contracts and, where applicable, service level agreements, must clearly specify at minimum:

- Confidentiality and non-disclosure requirements;
- The duration of the contract or agreement;
- Expectations regarding the third party's security controls, ensuring they appropriately mitigate the risks identified during the third party maturity assessment, and meet any security requirements mandated by legal and/or contractual obligations;
- Requirements associated with the ownership of intellectual property and data sovereignty as specified in the *Information Classification and Asset Management Policy*;
- Requirements to ensure background verification checks are performed either by the third party or PAE for all individuals who have access to 'RESTRICTED' PAE information and IT assets;
- Any additional third parties (fourth parties to PAE) relied on by the third party to deliver their services as part of the contract, and the obligations of the third party to ensure their third parties also meet the requirements of the contract;
- Requirements to notify PAE of any changes to services or fourth parties which may impact PAE;
- Resilience and recovery requirements based on the critical nature of the services provisioned by the supplier to PAE operations;
- Obligations to report and assist with the resolution of security weaknesses and/or incidents that impact the services and/or software provided by the supplier in a timely manner;
- Obligations to provide details of corrective actions planned to address identified security weaknesses and/or incidents that impact the services and/or software provided by the supplier in a timely manner;
- Liabilities in relation to damages that may be incurred by PAE as part of the relationship, including reputational, financial, compliance or contractual requirements;
- Any requirement for the return or disposal of PAE IT assets on termination of the contract; and
- Requirements regarding regular performance monitoring by way of service reports, review of records or a right to audit the third party in relation to their security requirements as defined by the contract or agreement.

APPENDIX M - SOURCES OF PRECURSORS AND INDICATORS

Precursors and indicators are identified using many different sources, with the most common being computer security software alerts, logs, publicly available information, and people.

Common sources of precursors and indicators for each category are shown in the following table

Source	Description
Alerts	
Intrusion Detection Prevention Systems (IDPS)	IDPS products identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces false positives - alerts that indicate malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources.
Security Information and Event Management (SIEM)	SIEM products are like IDPS products, but they generate alerts based on analysis of log data.
Antivirus and antispam software	Antivirus software detects various forms of malware, generates alerts, and prevents the malware from infecting hosts. Current antivirus products are effective at stopping many instances of malware if their signatures are kept up to date. Antispam software is used to detect spam and prevent it from reaching users' mailboxes. Spam may contain malware, phishing attacks, and other malicious content, so alerts from antispam software may indicate attack attempts.
File integrity checking software	File integrity checking software can detect changes made to important files during incidents. It uses a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected.
Third-party monitoring services	Third parties offer a variety of subscription-based and free monitoring services. An example is fraud detection services that will notify an organisation if its IP addresses, domain names, etc. are associated with current incident activity involving other organisations. There are also free real-time blacklists with similar information. Another example of a third-party monitoring service is CERT Australia – the national computer emergency response team who works with other Australian Government agencies and international CERTs, to provide Australian businesses with the best advice possible, as soon as possible.
Logs	

Operating system, service and application logs	Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs, such as recording which accounts were accessed and what actions were performed. Organisations should require a baseline level of logging on all systems and a higher baseline level on critical systems. Logs can be used for analysis by correlating event information. Depending on the event information, an alert can be generated to indicate an incident.
Network device logs	Logs from network devices such as firewalls and routers are not typically a primary source of precursors or indicators. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity. Still, they can be valuable in identifying network trends and in correlating events detected by other devices.
People	
People from within PAE	Users, system administrators, network administrators, security employees, and others from within PAE may report signs of incidents. It is important to validate all such reports. One approach is to ask people who provide such information how confident they are of the accuracy of the information. Recording this estimate along with the information provided can help considerably during incident analysis, particularly when conflicting data is discovered.
Community	Community complaints or feedback may provide indication of a security incident. This may be through a community member becoming aware of a breach of their personal information or if a customer finds their personal information displayed in a public space within PAE facilities. It is important to ensure information security is considered as part of the root cause analysis of community complaints or feedback.
People from other organisations	Reports of incidents that originate externally should be taken seriously. For example, PAE might be contacted by a party claiming a system at PAE is attacking its systems. External users may also report other indicators, such as a defaced web page or an unavailable service. Other incident response teams also may report incidents. It is important to have mechanisms in place for external parties to report indicators and for trained employees to monitor those mechanisms carefully. This may be as simple as setting up a phone number and email address, configured to forward messages to the help desk.
Other	
Network flows	A network flow is a communication session occurring between hosts. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts.
Publicly Available Information	Information that is readily available, through media for example.

Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in detecting and analysing new attacks. CERT Australia provides advice and support on information threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest. CERT is a single point of contact for information security issues affecting major Australian businesses. They work in the Information Security Operations Centre, sharing information and working closely with the Australian Security Intelligence Organisation (ASIO), the Australian Federal Police (AFP) and the Australian Cyber Security Centre (ACSC).
--	---

APPENDIX N – WORK INSTRUCTION ENROLLING SYSTEM USER

A task will be received in the DUTYITACCESS tasklist. It will be shown similar to below

New Starter Details for Action

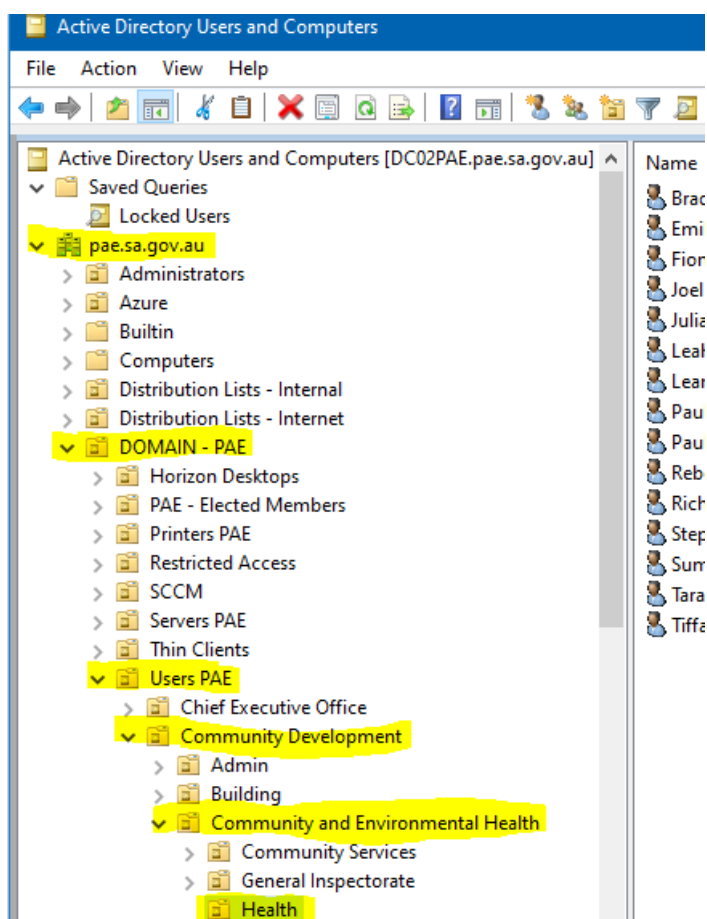
New Starter Details - 4190 - Community & Environmental Health Support Coordinator - Lily Francis

Temp On-boarding

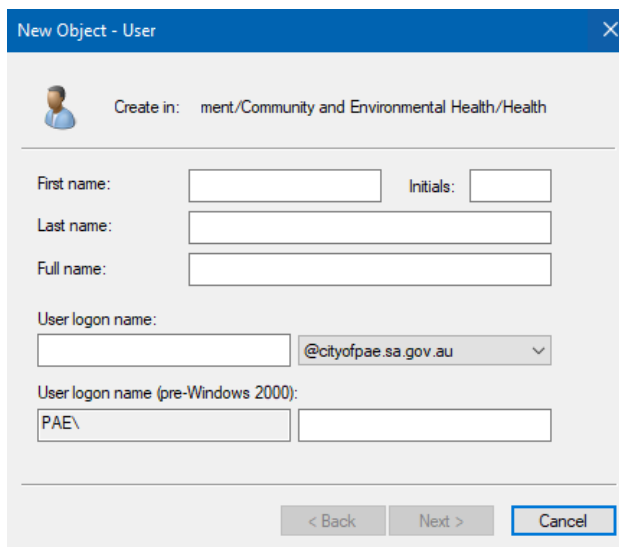
Request for Temp Access | Kayla Murray | 9044 - 28/02/2022

Create the user in Active Directory (AD)

To do this you need to find the relevant department. Then right-click on the team and select 'New > User'



The New Object – User form will pop up. Fill in the details, similar to below



New Object - User

Create in: ment/Community and Environmental Health/Health

First name: Initials:

Last name:

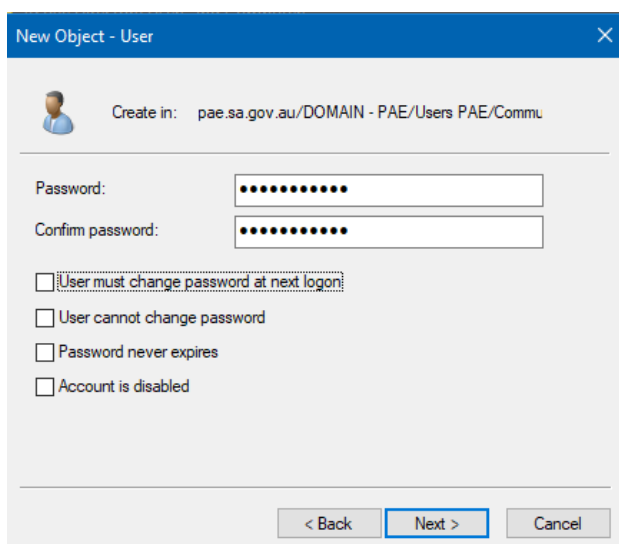
Full name:

User logon name: @cityofpae.sa.gov.au

User logon name (pre-Windows 2000):

< Back Next > Cancel

Set the Password – Untick the change password at the next logon (This is required for desktop setup)



New Object - User

Create in: pae.sa.gov.au/DOMAIN - PAE/Users PAE/Commu

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

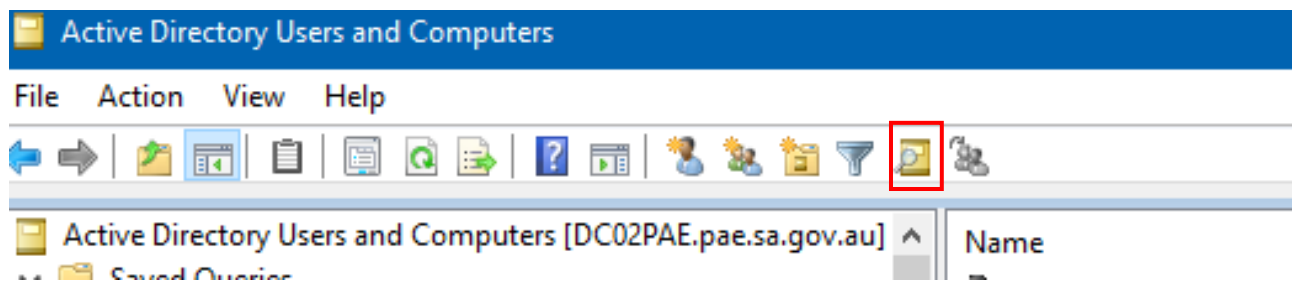
☐ Password never expires

☐ Account is disabled

< Back Next > Cancel

Select Next, then Finish

Find User in AD by using the search function.



Fill in the details, starting with the General tab, then Apply.

Organization		Published Certificates		Member Of
General	Address	Account	Profile	Telephones
Jennifer Reid				
First name:	Jennifer	Initials:		
Last name:	Reid			
Display name:	Jennifer Reid			
Description:	User Staff Jennifer Reid			
Office:	Civic Centre			
Telephone number:	6994	Other...		
E-mail:				
Web page:		Other...		
OK Cancel Apply Help				

Then the Organisation tab, Apply.

Jennifer Reid Properties ? X

Password Replication	Object	Security	COM+	Attribute Editor
General	Address	Account	Profile	Telephones
Organization	Published Certificates		Member Of	

Job Title: Environmental Health Officer

Department: Community Development

Company: City of Port Adelaide Enfield

Manager

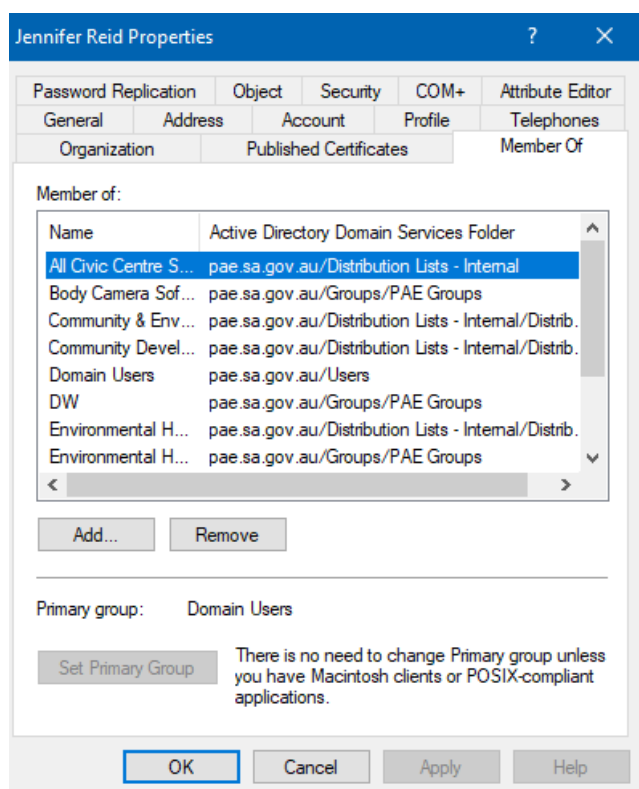
Name: Summa Bragg

Change... Properties Clear

Direct reports:

OK Cancel Apply Help

Then the Member Of tab,



Groups that are usually added in here (it can help to find someone in a similar position)

G: Drive (Corporate Services, Community Development or City Assets)

Distribution Groups relevant to the position

VDI Dedicated

Phriendly Phishing

Once changes are made, Select Apply, and close.

Creating a user in Technology One Core Enterprise (CES)

Go to System Tab > Access Control > Users. Right-click on Users and select 'Add Users'



Fill in the form details and save

User

User ID:*

External Authentication Details

Each user may optionally have an Alias User ID that is longer than their User ID. This is compared against the User Name they enter when logging in. This is compared against the User Name they enter when logging in. This is compared against the User Name they enter when logging in.

Alias User ID:

Name

Title:

First Name:

Last Name:

Narration:

User Type:*

Contact Details

Department:

Phone:

Fax:

Email Address:

Access Details

The User Status indicates whether the New User is awaiting configuration by the System Administrator; or already has their Access Assigned.

User Status:* ☐ Account Disabled

Account Start Date/Time:

Account End Date/Time: Account End Reason:

Last Login:

User Group:* Default User Group

Assigned Access

Roles can not be effective at the same time as a User Profile. Only one User Profile may be active at a point in time.

Access Method Code*	Name*	Description	Effective Date	Expiry Date
▶ User Profile with Assign...	4209-POSITION-PROFILE	Position 4209 - Port Adelaide Enfield Profile	19/10/2021	14/01/2022

Creating a user in Technology One Property & Rating (P&R)

Go to System Tab > Access Control > Users. Right-click on Users and select 'Add Users'

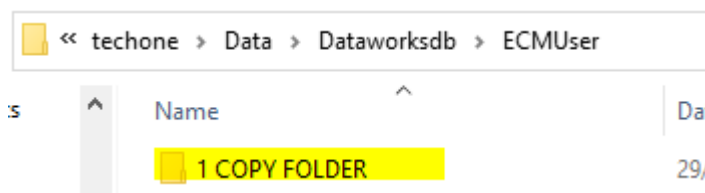


Fill in details, similar to above, Save.

Creating a User ECM Cache

If the user is an ECM user, they will need an ECM Cache Folder.

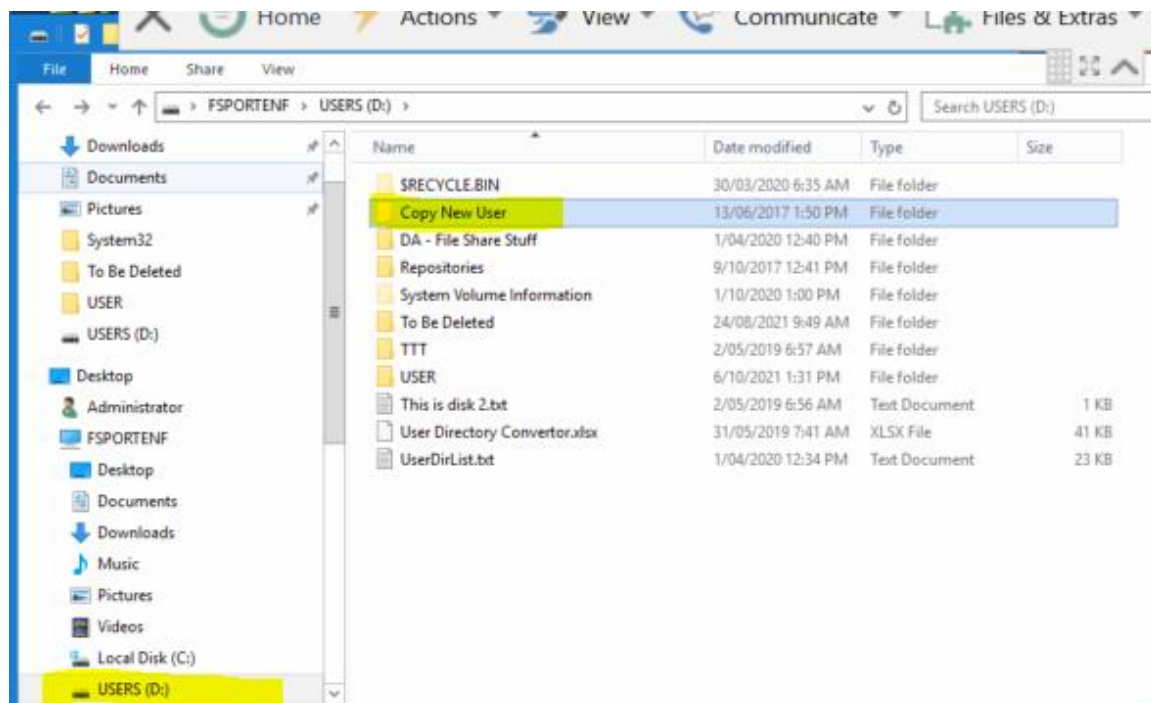
These can be found here: <\\pae.sa.gov.au\techone\Data\Dataworksdb\ECMUser>



Copy folder and paste then title it FIRSTNAME.LASTNAME (JOHN.SMITH)

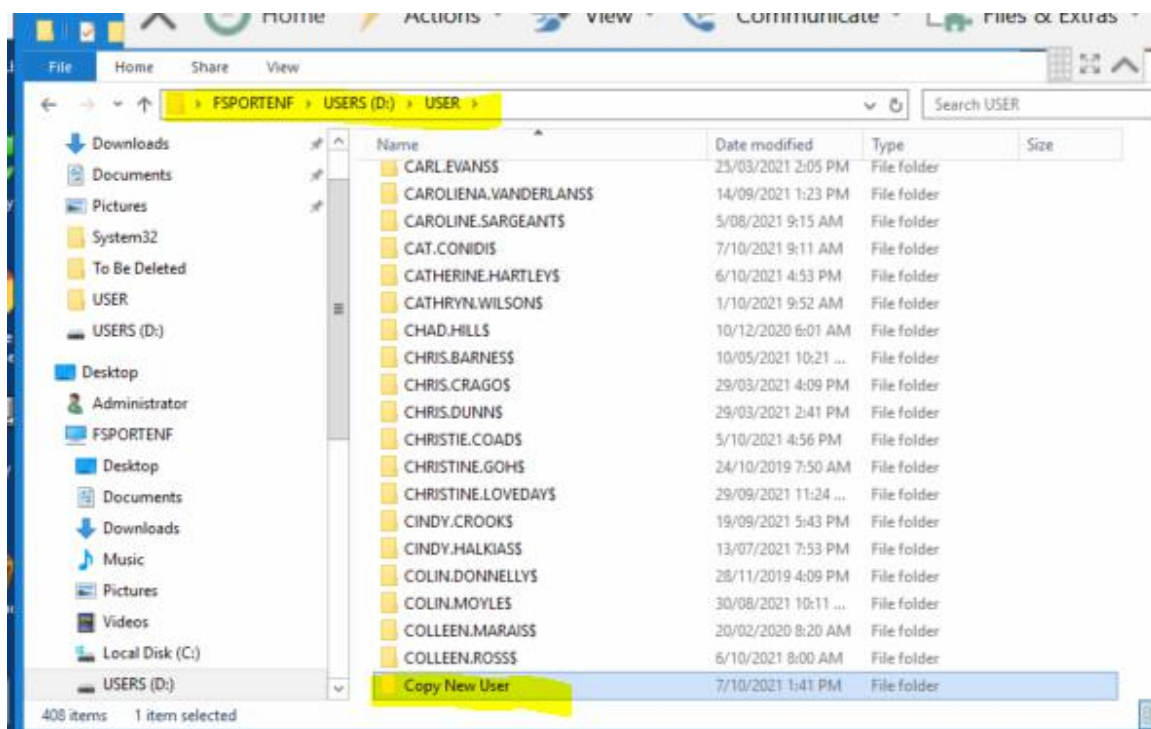
Creating a User H Drive

Go to <\\fsportenf>, Go to Users Folder and copy 'Copy New User'

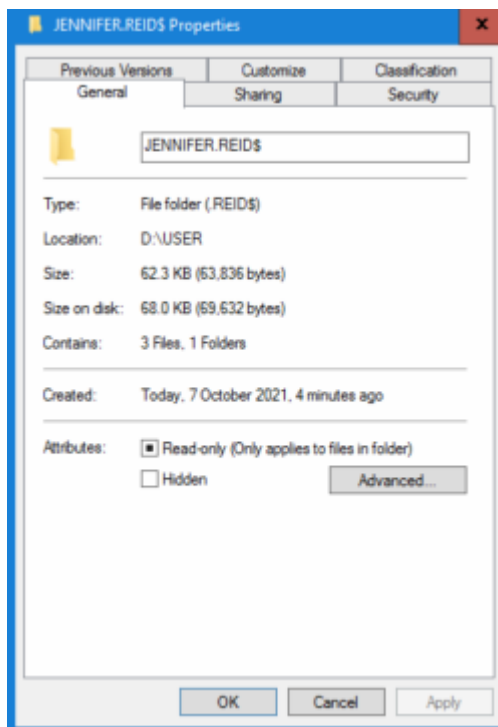


Double Click 'User' to open and paste 'Copy New User'

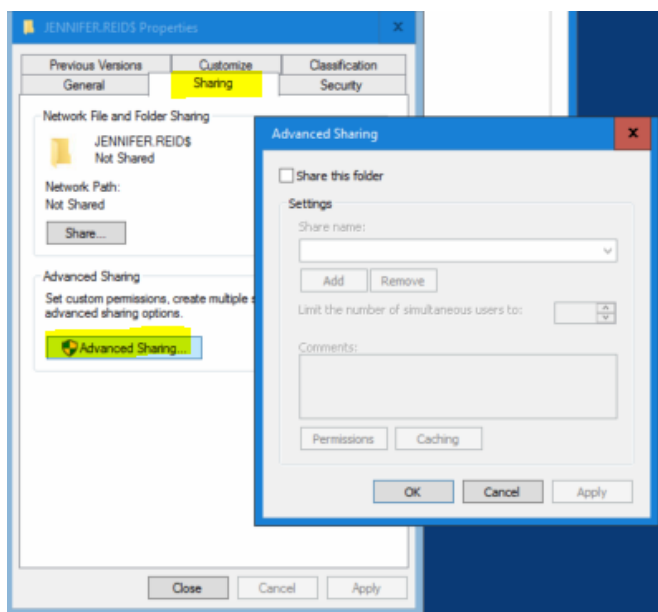
Rename to FIRSTNAME.LASTNAME\$ (JOHN.SMITH\$)



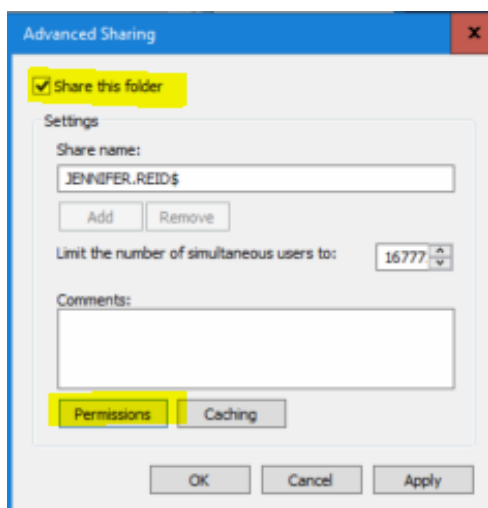
Right Click and Select Properties



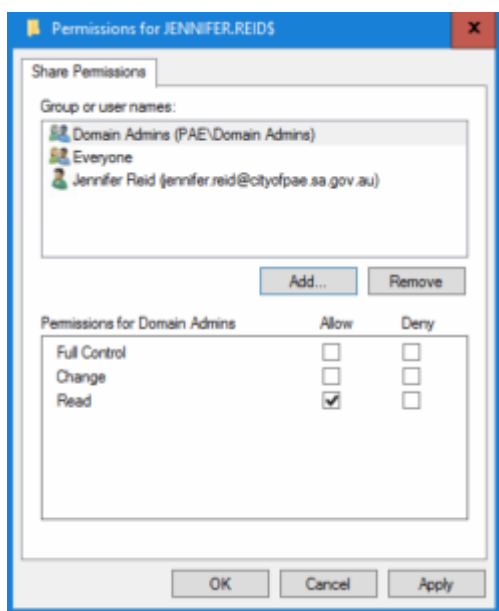
Select Sharing tab and then Advanced Sharing



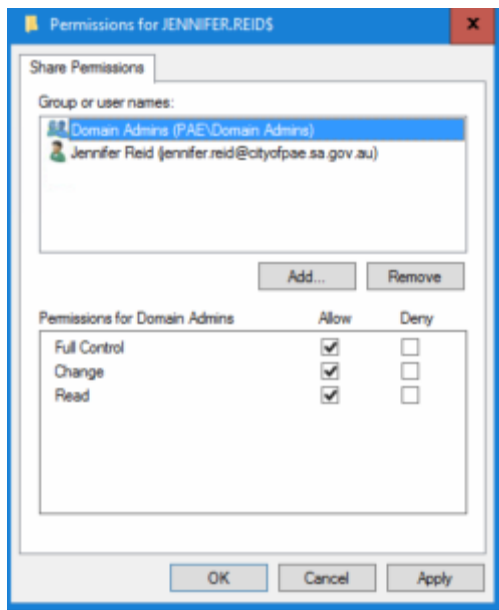
Tick Share this Folder and Apply. Then Select Permissions



Select Add and Add User and Domain Admins. Select Apply then Remove Everyone.

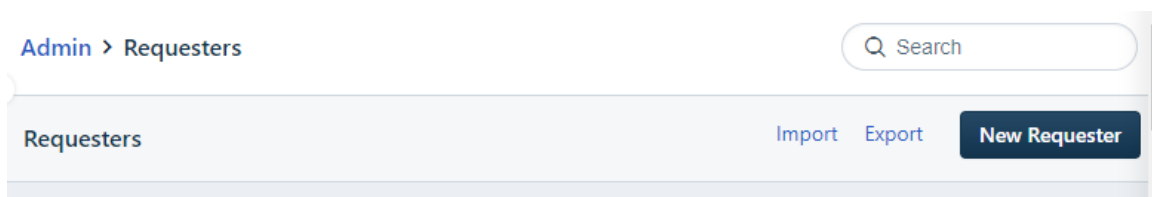


Select users one at a time, then tick Full Control



Creating User in Fresh Service

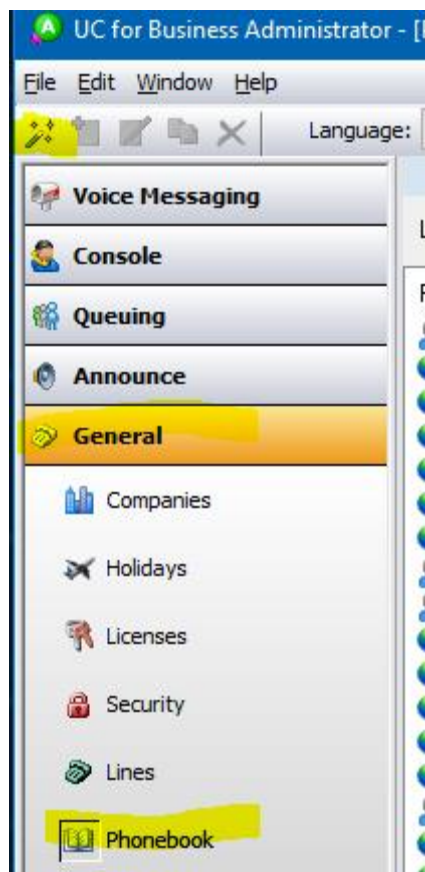
Go to Admin > Select Requesters, then fill in details but do not create a 2nd email address



Creating User in QM Phonebook

User Administrator software located [\\Vucbsrv\cti\bin\Administrator.exe](http://Vucbsrv\cti\bin\Administrator.exe)

Go to General > Phonebook > Select Wand



Fill in Details then select Next

The screenshot shows a dialog box titled "Adding Phonebook Contact" with a close button (X) in the top right corner. The main heading is "Enter the Contact Name". Below it, a subtitle reads "Enter the first and last name of the new contact to add to the Phonebook .". There are two input fields: "First Name:" containing the text "Jennifer" and "Last Name:" containing the text "Reid".

Select PAEC and then Next

This screenshot shows the same dialog box as before, but the "Next >" button at the bottom is highlighted with a yellow rectangle. Above the buttons, a dropdown menu is open, showing "PAEC" as the selected option.

Add extension number (and mobile if the user has one), then Next

The screenshot shows the "Adding Phonebook Contact" dialog box at the "Enter the Contact Details" step. The subtitle is "Enter the Contact Details". The "Extension:" field contains "6994" and is highlighted with a yellow rectangle. Below it is a "Skype Address: sip:" field. There are several rows for phone numbers, each with a dropdown menu set to "Australia (61)" and two input fields: "Business:", "Home:", "Mobile:", "Fax:", and "Pager:". The "E-mail:" field is at the bottom.

Select Basic User, then Next, Next, Next and Finish

The screenshot shows the "Adding Phonebook Contact" dialog box at the "Select the Security Class" step. The subtitle is "Select which Security Class to assign to the new contact to.". A list of security classes is shown in a scrollable area: "Administrator", "PAEC: Administrator", "PAEC: Agent", and "PAEC: Basic User". The "PAEC: Basic User" option is selected and highlighted with a blue background.

Employee number and logon name needs to be added here

Editing Contact 'Deni Freebairn' [1147] ✕

General Numbers/Addresses Advanced Additional Info

Fields

Field	Value
Field Name	
Show on the Phone	
User Logon Name	deni.freebairn
Employee ID	55854

Fields Editor...

OK Cancel Apply Help

CHECKLIST FOR CREATION OF NEW USER

1.	User in Active Directory
	☐ User added to AD. Username assigned: _____
2.	User's details
	☐ General details added to Active Directory
	☐ Organisational details added to Active Directory
3.	AD Groups assigned
	☐ G Drive
	☐ Distribution Groups
	☐ VDI Dedicated
	☐ Phriendly Phishing
	☐ Other _____
Reason for any variation:	
4.	Technology One
	☐ Property and Rating
5.	H Drive
	☐ Permission correct
6.	Fresh
	☐ User created
7.	QM Phone Book
	☐ User created
	☐ Employee Id added as attribute
	☐ Mobile number added
8.	User's password set to require change at first login

CHECKLIST FOR SEPERATION OF USER

1.	User in Active Directory. Username _____
	☐ User set to inactive in AD.
2.	User's details
	☐ General details added to Active Directory
	☐ Organisational details added to Active Directory
3.	AD Groups removed
	☐ G Drive
	☐ Distribution Groups
	☐ VDI Dedicated
	☐ Phriendly Phishing
	☐ Other _____
Reason for any variation:	
4.	Technology One
	☐ Property and Rating expired
6.	Fresh
	☐ User disabled?
7.	QM Phone Book
	☐ User removed

APPENDIX O – WORK INSTRUCTION ACCESS REVIEW

Access Review	Frequency	Procedures	Responsibility
Users not logged in	Monthly – First of the month	Run this report http://appspae:8080/Reports/Pages/Report.aspx?ItemPath=%2fIT%2fT001_6+User+Last+Logon&ViewMode=Detail for the 'All Users' AD Group Review the report with a specific focus on finding users who should be removed from Council's systems. At a minimum check; • Users who have never logged in; • Users who haven't logged in for more that 30 days • Users who an inactive in HR Share this report with Payroll Officer and request the same review.	IT Operations – Team Member
		Run this report http://appspae:8080/Reports/Pages/Report.aspx?ItemPath=%2fIT%2fT001_6+User+Last+Logon&ViewMode=Detail for the 'Separated Users' AD Group Review the report with a specific focus on finding users who have logged after separation. At a minimum check; • Last login vs termination date	IT Operations – Team Member

		Run this report http://appspae:8080/Reports/Pages/Report.aspx?ItemPath=%2fIT%2fIT001_6+User+Last+Logon&ViewMode=Detail for the 'Special Generic' and 'PAE Corp Generic' and 'Special Service' AD Groups Review the report with a specific focus on finding users who should be removed from Council's systems. At a minimum check; • Users who have never logged in;	IT Operations – Team Member
		Create a Fresh Service Ticket, add the reports and any notes about proposed actions taken and observations.	IT Operations – Team Member
		Obtain approval from the Team Leader – IT Operations to execute the proposed changes.	IT Operations – Team Member
		Review proposed changes and approve or deny.	Team Leader – IT Operations
		Execute the approved changes and add notes to the Fresh Ticket	IT Operations – Team Member
Privileged Users		Run this report http://appspae:8080/Reports/Pages/Report.aspx?ItemPath=%2fIT%2fIT001_6+User+Last+Logon&ViewMode=Detail Review the report with a specific focus on finding users who should not be Domain Admins.	IT Operations – Team Member

		Create a Fresh Service Ticket, add the reports and any notes about proposed actions taken and observations.	IT Operations – Team Member
		Obtain approval from the Team Leader – IT Operations to execute the proposed changes.	IT Operations – Team Member
		Review proposed changes and approve or deny.	Team Leader – IT Operations
		Execute the approved changes and add notes to the Fresh Ticket	IT Operations – Team Member
Key Applications – Admin users	Quarterly; Feb, May, Aug and Nov.	Run the Report http://appspae:8080/Reports/Pages/Report.aspx?ItemPath=%2fFinanceOne%2fFIN026_2+Access+to+Core+Enterprise+Suite+by+User&ViewMode=Detail Select the roles; • CPM Administrator, • PAE- System Administrator – Budgeting, • PAE- System Administrator – CPM, • PAE- System Administrator – Finance, • Payroll Administration, • System Administrator – CPM, • System Administrator – Supply Chain For All Departments.	IT Operations – Team Member
		Review the results for any unusual access. Share the report and observations with Managers; Finance, People and Culture, Strategy and Performance, Infrastructure Asset Maintenance, Corporate Information and request confirmation of actions (including do nothing).	Team Leader – IT Operations
		Create a Fresh Service Ticket, add the reports and any notes about proposed actions taken and observations	Team Leader – IT Operations

		Execute the approved changes and add notes to the Fresh Ticket	Team Leader – IT Operations
Key Applications – all users	Annually – July	Run the Report http://appspae:8080/Reports/Pages/Report.aspx?ItemPath=%2fFinanceOne%2fFIN026_2+Access+to+Core+Enterprise+Suite+by+User&ViewMode=Detail Select all roles and (for ease of review) one Department at a time	IT Operations – Team Member
		Review the results for any unusual access. Share the report and observations with Directors and request confirmation of actions (including do nothing).	Team Leader – IT Operations
		Create a Fresh Service Ticket, add the reports and any notes about proposed actions taken and observations	Team Leader – IT Operations
		Execute the approved changes and add notes to the Fresh Ticket	Team Leader – IT Operations

APPENDIX P – IT OPERATIONS START OF DAY CHECKLIST (BACKUPS, SERVERS, AND APPLICATIONS)

START of DAY PROCEDURE

Start of Day usually involves two IT Operations Team members to be available by 7 am Monday to Friday (excluding Public Holidays) to check overnight Backups, SQL Jobs, Systems Availability and Capacity.

The IT Duty Officer who is on-call on the weekend is required to assume the same checks for the mornings they are on-call.

Backup Routine

Staff member to

- Check that the Veeam Backups have occurred overnight and attempt to resolve any failed jobs.
- Check all the overnight Microsoft SQL Agent Jobs have run successfully and if possible, re-run any failed jobs otherwise report the error through the Fresh Service Desk and assign it to the appropriate Agent.
- Complete the manual Daily Backup Log which marks Jobs as succeeding or failing.
- Rotation of the weekly and monthly backup tapes ready for off-site storage.

Systems Availability and Capacity

Staff members to follow the checklist below.

Category	Check	Notes
LOGON and NETWORK CHECK	Logged On successfully	MUST READ NOTE Do not start any of the following applications listed below in this section before you have first completed all the Systems and Server Availability and Capacity Checks. • ECM • Outlook • Technology One CES • Technology One P&R Why – because if you start ECM first and then a dependant server for ECM such as DASECM-PRO has to be rebooted during your checks then you are not truly checking the logon experience of a user as the DAS Service is already started on your PC.

		Once you have completed all your checks and you start the listed products below in this section then your experience should be close to that of a user.
DRIVE MAPPING CHECK	Check you have at least the following mapped drives (G:, H, and W:).	
LOCKED ACTIVE DIRECTORY ACCOUNTS CHECK	Check for Locked Accounts – investigate and only unlock what is required to ensure systems are functioning.	Locked Users should either Self-Serve to unlock or call and sufficiently identify themselves before unlocking their accounts
CORE APPLICATIONS RUN FROM INTRANET CHECK	Start-up Intranet • Customer Requests • IT Service Desk • IPS (Hansen) • CIAnywhere • Internet Connection Check	Customer Request Note: If application starts up and that you can pull down a Category then probably ok, but- if this does not work it is a fair indicator that you need to go to the TECHNOLOGY ONE-ECM section on this check list for the and check the servers DASECM-PRO or Log files are full on the DWPordenf. IT Service Desk Note: as this is Hosted you can use this also as the Internet Connection Check) Internet Connection Check Note Go to an external Web site this will confirm that we have Internet Access.
PREPARING TO PERFORM SYSTEMS AVAILABILITY AND CAPACITY CHECKS	Startup Teamviewer as you may prefer to use this to check most of the servers	Note: From now on in these instructions you may be swapping between Teamviewer and vSphere Client depending on what you are doing and what is the easiest for you. e.g. Capacity Checks and Power Off or Restart through Teamviewer and Powered Up Status and Powering On through vSphere .
		vSphere Client Connect to VMWare browse using the URLs https://cpaevdivc01/ or https://cpaecivvc01/ and proceed through trust messages and then select Launch vSphere Web Client (HTML5)

DATASTORES	Check status of Datastores to ensure no errors	
	Check Free Capacity of each Datastore	
HOSTS	Check Hosts if they are all Powered On and available, if not confirm with Darren if known issue	
	Check for any Alarms (check what the Alarm says).	
VMs (Guest Servers)	Check for any Alarms (check what the Alarm says)	
	Check Powered On and for any Powered Off that should be on	
DOMAIN CONTROLLERS	Open Console for each Domain Controller and perform a check on e.g. Tasks etc to ensure that the server is not frozen and is running	Using either Teamviewer or vSphere Client
CHECKING SPECIFIC GUEST SERVER	Microsoft Updates	Be Careful and give consideration whether to progress with installation (more guidance is required with this area due to outcome of Security Review 2021). If proceeding with an installation which requires a Restart first check or inform Depot staff and any obvious Civic Centre staff who are in during the 7am to 7.30am timespan that a reboot is required otherwise wait until next day for reboot.
SQL TASKS AND SERVERS REQUIRING REBOOTS		If rebooting any server that is a SQL Server, check that it is not running any SQL Tasks, due to the number of inter-SQL Server dependencies at the same time, also check SQL Tasks on APPSPA, CIPortenf, DWPPortenf, Bookpae and HEPortenf.

		• If they are running Tasks check the history of the Task to see how long it takes if it needs to be re-run. • Check whether the Task Description indicate if it links to the server that is requiring a reboot e.g. check the description of the Task to see whether it indicates it is rebuilding something such as an ECM Index which would not be ideal to cancel. • Many Reports or OLAP Tasks can be re-run if they only take a short time, Tasks that take many hours need more consideration or check with an Analyst.
GUEST SERVERS SERVICES, CAPACITY AND PERFORMANC E		Generally for convenience these checks are done in Teamviewer
CAPACITY – OVERVIEW	Check is to identify and resolve capacity issues.	The purpose of this check is to identify and resolve capacity issues and resulting outages or consequences. At a minimum check Capacity of Disks of all servers you visit as part of the daily check. There is more Capacity Related checking dealt with under the heading CAPACITY CHECK - OTHER Also Teamviewer can indicate a Capacity Issue and that needs to be investigated.
TECHNOLOGY ONE - CES, CIANYWHERE AND PROPERTY & RATING	Open Console for CIPortenf	CHECK • Disk Capacity • Task Manager – ensure T1.Tb.Dp.Server.App.exe *32 is running and monitor for a few minutes to check that T1.Tb.Dp.Job.App.exe *32 are running or start up during your period of observation. If not running or problem (e.g. frozen and Memory usage not changing) then go to Service and start T1 ci Distributed Processor and start or restart the service depending on situation. If you have to restart CIPortenf then check DPSCProd (If this server is not rebooted at least restart the Distributed processor after the CIPortenf reboot)

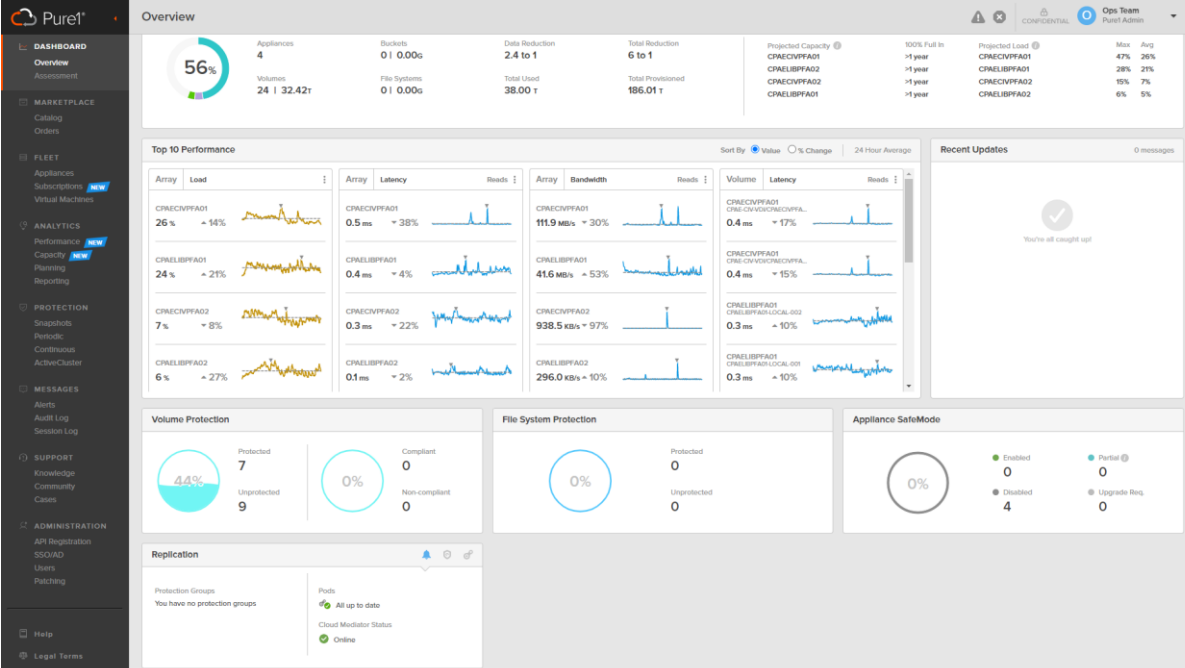
		Check email is working – open Outlook and send an email to t1connect-prod@portenf.sa.gov.au with #ping in first line of body of email, no Subject required (same applies for test substitute t1connect-prod with t1connect-test).
	Open Console for DPSCProd	CHECK - Task Manager – Services ensure T1 ci Distributed Processor is running and under Processes monitor for a few minutes to check that instances of T1DistributedProcessor.JobRunner start up during your period of observation. If not running or problem (e.g. frozen and Memory usage not changing) then go to Service and start T1 ci Distributed Processor and start or restart the service depending on situation. - Task Manager – Services ensure T1ServerAgent Service is running. *Important Note DPSCProd must be running for the CS DFS Namespace to be available This is the equivalent of the old T1 Share for CS (not applicable for Property & Rating which is still a Share) DFS Namespace is llpae.sa.gov.au/techone which is managed through Active Directory and a link to the management console is on DPSCProd
	Open Console for APCIAProd	Task Manager – Services ensure T1ServerAgent Service is running
TECHNOLOGY ONE - ECM	Open Console for DWPortenf	Note this is ECMs Database Server only Server logged on as paeladministrator. CHECK Disk Capacity Check Disk Capacity NOTE: It is usually the D: Drive (SQL Log Files) that fills up. <i>(More instructions are required to deal with this as the SQL Log Files need to be shrunk)</i>

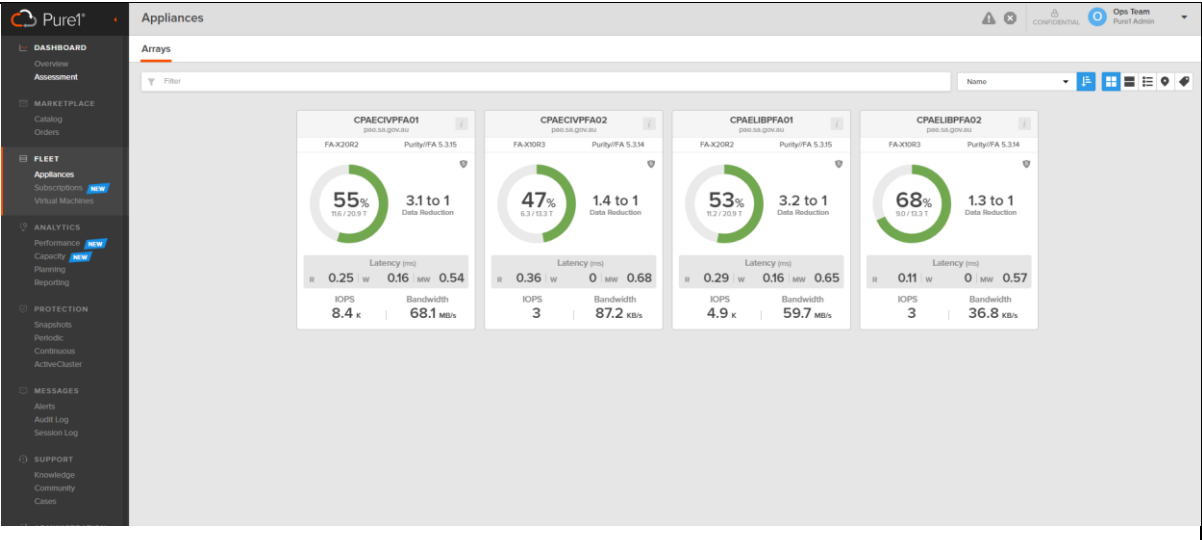
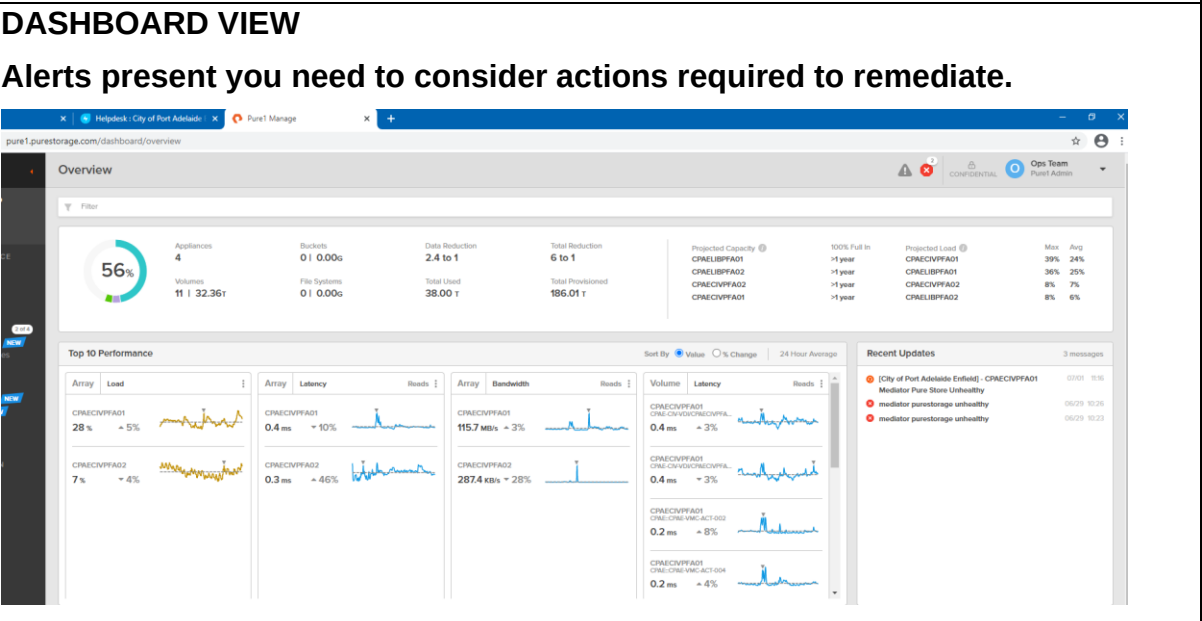
	Open Console for ECMinCache	Note this is ECMs InCache File Server only Server logged on as paeladministrator. CHECK • Disk Capacity
	Open Console for DPECMDEF-PRO	Note this Renders new documents Server logged on as t1_service. CHECK • Task Manager (Services) – ensure t1distproc is running. • Task Manager (Services) – ensure T1Server Agent is running. • Task Manager (Services) – ensure T1 ECM Rendering Manager is running as this Renders Action Index Tasks into PDFs • In your Internet Browser go to http://dpecmdef-pro:32249/showstatus if does not show log with various DP Processes then check IIS Manager DPECMDEF-PRO is running (logged on as t1_service)
	Open Console for DPECMRENCC-PRO	<i>Note this does Backlog Rendering for CIAnywhere This DP Service runs the Distributed Processor Jobs for Connected Content (including new Customers) which are created / registered from Property and Rating into ECM. This server logged on as t1_service.</i> CHECK • Task Manager (Services) – ensure t1distproc is running. • Task Manager (Services) – ensure T1Server Agent is running.
	Open Console for DASECM-PRO	<i>Note this is the DAS Server also deploys ECM Smart Client and Councils customised on-line apps (including Customer Requests) This server logged on as t1_service.</i>

		CHECK • Task Manager (Services) – ensure T1Server Agent is running • Task Manager (Services) – ensure there are 6 occurrences of Zope are running • IIS Manager that DASECM-PRO is running (logged on as t1_service) • IIS Manager that Application Pools a. ECMProxy is started b. T1ECMProdDeploy is started (Identity is t1_service) c. DataworksWS is started (Identity pae\administrator) Note: The DataworksWS provides the functionality for Customer Requests and on-line Services (Council's customised). • To check relevant operations are running from your Browser go to http://dasecm-pro/DataWorksWS/DataWorks.aspx Important Notes for DASECM-PRO A. <i>The Application Pools must be running for users to be able to logon</i> B. <i>Zopes are stopped by a Scheduled Task every night and are then restarted by another Scheduled Task.</i> BATCHES TO MANUALLY MANAGE ZOPE <i>There is a batch to stop Zope under</i> C:\ECM\Zope\all_stop_service_DWECMProd.bat <i>There is a batch to start Zope under</i> C:\ECM\Zope\all_run_service_DWECMProd.bat C. <i>Reports are run as a Scheduled Task every day if not run then check log under C:\ECM\WFReport</i>
	SHUTDOWN AND RESTART OF ECM SERVERS	Important Note:

		Rarely are we required to perform the following Shutdown and Restart / Power-On Process on DWPORTENF (Database server) and ECMINCACHE server but if required then follow the order below. More commonly if documents are not being rendered or Connected Content is not going into ECM or all users are having trouble logging into ECM then you follow the order below but skip DWPORTENF and ECMINCACHE. Generally, Start up is in the reverse order of Shutdown.
	SHUTDOWN ORDER FOR ECM SERVERS	1. DPECMDEF-PRO (running ECM workflow server, Legacy Rendering Server and DP Primary Server). 2. DPECMRENCC-PRO (DP Secondary server running Backlog rendering and Connected Content). 3. DASECM-PRO (DAS server). 4. DWPORTENF (Important Note: Rarely require Shutdown if problem is related to User Logons or Distributed Processing issues). 5. ECMINCACHE (Important Note: Rarely require Shutdown if problem is related to User Logons or Distributed Processing issues).
	RESTART and POWER-ON ORDER FOR ECM SERVERS	1. ECMINCACHE (Important Note: Rarely require Shutdown and Power-On if problem is related to User Logons or Distributed Processing issues). 2. DWPORTENF (Important Note: Rarely require Shutdown and Power-On if problem is related to User Logons or Distributed Processing issues). Please make sure the SQL server is fully up and running before starting the other servers. 3. APCIAPROD – Restart Required. Note the Restart of the CiAnywhere server will impact all of CiAnywhere including CES, restarting this server needs consideration of impact or if the issue requiring reboot had already been resolved. 4. DASECM-PRO (DAS server).

		5. DPECMRENCC-PRO (DP Secondary server running Backlog rendering and Connected Content). 6. DPECMDEF-PRO (running ECM workflow server, Legacy Rendering Server and DP Primary Server).
IPS - INFOR PUBLIC SECTOR – IPS (formerly Hansen)	Open Console for HEPortenf	CHECK • Disk Capacity • Data Services Framework is running, this is set under Scheduled Tasks to restart each day at 12:00AM Note: Although rarely required to be run the Data Services Framework can be manually restarted from the HEPORTENF from D:\Admin\Scripts\Restart DSF.bat.
CAPACITY CHECK – OTHER	Also check Disk Capacity for • FSPortenf • BookPAE • APPSPA • MXP • PAE-DFS01	
PURE STORAGE DAILY CHECK - HEALTHY STATE	To Logon to Pure1 browse to URL https://pure1.purestorage.com using the logon credentials and password as per our Security Documentation. This will then present you with Pure1 and a menu is displayed on the left hand side of the screen the most common used for the purpose of the PURE STORAGE DAILY CHECK	(To see example of errors refer PURE STORAGE DAILY CHECK - UN-HEALTHY STATE)

	are DASHBOARD and FLEET.	
DASHBOARD VIEW	CHECK Top right corner there are no Alerts Recent Updates is not showing any Alerts	 The screenshot displays the Pure1 dashboard interface. On the left is a dark sidebar with navigation links: DASHBOARD (Overview, Assessment), MARKETPLACE (Catalog, Orders), FLEET (Appliances, Subscriptions, Virtual Machines), ANALYTICS (Performance, Capacity, Planning, Reporting), PROTECTION (Snapshots, Periodic, Continuous, Active-Cluster), MESSAGES (Alerts, Audit Log, Session Log), SUPPORT (Knowledge, Community, Cases), and ADMINISTRATION (API Registration, SSO/AD, Users, Patching). The main content area is titled 'Overview' and includes a top summary bar with metrics like Appliances (4), Volumes (24), Backups (0), and Data Reduction (2.4 to 1). Below this is a 'Top 10 Performance' section with charts for Load, Latency, Bandwidth, and Volume for various appliances. Further down are 'Volume Protection' and 'File System Protection' status sections, and a 'Replication' section at the bottom. On the right side of the dashboard, there is a 'Recent Updates' panel showing a checkmark and the message 'You're all caught up!'.

FLEET VIEW - Appliances	CHECK Both Civic and the Port Adelaide Library side of the Pure Storage are showing and no obvious errors.	
PURE STORAGE DAILY CHECK - UN-HEALTHY STATE		DASHBOARD VIEW Alerts present you need to consider actions required to remediate. 

		Top right corner there are Alerts <i>PURE STORAGE DAILY CHECK - UN-HEALTHY STATE</i> Recent Updates is showing Alerts <
--	--	--

