Western Parkland City Authority

Cyber Security Policy

Final June 2022

wpca.sydney

NSW GOVERNMENT

Document control

Document Type(s) *(Tick all boxes that apply)*	☒ Policy ☐ Procedures ☐ Guideline ☐ Fact sheet	
Policy category	Information, Communications and Technology	
Responsible Business Unit	Corporate Services	
Document Owner	Director Corporate Services	
Publication	☐ Not for publication ☒ Intranet	☐ WPCA website ☐ Other: (please specify)
** The Government Information (Public Access) Act 2009 (the GIPA Act) requires that all of the Department's current policy documents be made available on this website (unless there are overriding public interest reasons why that should not be done). WPCA Legal Branch can provide advice.*		

Document approval

Version	Objective ID	Name & Position	Signature	Date	Effective Date
1.1	A5370728	James Hebron		05/07/2022	

Document version control

Version	Objective ID	Status	Date	Prepared By	Comments
V1.0	A5370728	Draft	May 2022	Virginia Tinson	
V1.1	A5370728	Final	June 2022	Virginia Tinson	Revised following ARC feedback.
V1.2	A5370728	Final	Oct 2022	Virginia Tinson	Revised following ARC feedback.

Review date

The Authority will review this policy every two years or more frequently if required. It may be reviewed earlier in response to a change in the Australian Government or NSW Cyber Security guidelines.

Contents

1. Policy Statement

Western Parkland City Authority (WPCA) recognises that information and associated systems/applications are a key asset and must be securely protected. Therefore, it is WPCA's Policy to ensure that all WPCA information and key assets, including but not limited to its personal and sensitive information and information assets, are properly safeguarded within a secure environment.

WPCA's information exists in many forms, such as:

- Data is stored in external systems managed by Third Party Service Providers (TPSP), multi-tenant cloud platforms, and general software as a service (SaaS) platforms.
- Data stored on computer disks and other storage media;
- Data transmitted across the networks;
- Information printed or written on paper; or
- Spoken in conversations in person or over the telephone.

Protection of information and Information and Communication Technology (ICT) systems is essential for WPCA to maintain its reputation as a trusted and respected government organisation. This document sets the direction for WPCA cyber security and information technology security, describing the intentions, principles, and requirements to:

- Protect the Confidentiality of WPCA information;
- Protect the Integrity of WPCA information; and
- Protect the Availability of WPCA information.

The NSW Cyber Security Policy requires that agencies implement a Cyber Security Framework (or equivalent) that covers at least the agency's crown jewels. WPCA has aligned its Cyber Security policy to the Cyber Security NSW policy and has therefore chosen to align with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The NIST CSF is a framework that integrates industry standards and best practices to help organisations manage cyber security risks. The NIST CSF core functions are: IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER. This policy guides how the WPCA information, communication systems and technologies are protected through the implementation of approved security controls and various security standards.

2. Scope

This policy applies to—

- All personnel employed by WPCA; any person or organisation contracted to or acting on behalf of WPCA; and any person or organisation employed to work on WPCA premises or facilities and all activities of WPCA.
- All information and information system assets are owned or outsourced by WPCA at all its business locations, regardless of format or storage device, and whether shared or allocated to individuals.

Information and information systems encompass technology, application systems and data.

The intended audience for this document is all users who have access to WPCA information or the systems and assets used to process, store or communicate that information.

3. WPCA Cyber Security Policy

The purpose of this policy is to:

- Provide a cyber security documentation framework to establish appropriate standards, processes, procedures and guidelines to support the implementation of the cyber security requirements across WPCA.
- Establish the minimum requirements for effectively managing cyber security across WPCA in a risk-based manner.
- Reduce the risk to WPCA information assets, including sensitive information that may be lost, corrupted, inappropriately used or disclosed.
- Provide clear direction to employees, contractors, service providers and external parties to understand their requirements to protect WPCA information assets from inappropriate use, modification, loss or disclosure.
- Provide guidance to identify, assess and manage areas of non-compliance to the WPCA cyber security policy to manage risks to the WPCA information assets.
- Promote and support adherence to appropriate legislation, regulation and industry standards.

Appropriate security standards and measures must be established, implemented, monitored, reviewed, and improved to ensure that WPCA's Cyber Security Framework and its business objectives are met.

The implementation of this Policy and the standards, processes, and procedures support the appropriate security measures to ensure compliance.

3.1. Acceptable Use

The WPCA Acceptable Usage Policy defines the appropriate use of computing and communications resources. It addresses the information stored on or transmitted via WPCA computers, networks, telephones and other communications devices.

Staff, contractors and consultants that have access to WPCA data must adhere to the security requirements of information systems and assets they use at all times. Reasonable precautions must be taken by staff to safeguard information systems and assets against inappropriate or unauthorised access. In particular:

- WPCA's information systems and assets must be used primarily for business purposes, in line with this Policy and any other related agreements/contracts.
- Staff must not access sensitive or security classified information unless there is a valid business requirement.

This section must be referenced in conjunction with the WPCA Acceptable Use Policy.

3.2. Cyber Roles and Responsibilities

To establish a management framework for the implementation and operation of cyber security and to assign roles and responsibilities for the management of cyber security, WPCA ensures:

- All cyber security responsibilities are defined and allocated.

- Responsibilities for the protection of individual assets and for carrying out specific security processes are identified.
- Responsibilities for information security risk management activities and, in particular, for acceptance of residual risks are defined.
- WPCA Board and executive management has the overall responsibility for cyber security within the organisation.
- All WPCA personnel are responsible for complying with the principles and policies in this Policy and standards where relevant to their jobs.
- Any person failing to comply with the security policies and standards could be subject to specified disciplinary actions.

All WPCA employees, contractors, and consultants	Are familiar with and comply with all WPCA Corporate Policies including this Cyber Security Policy and associated Standards and other corporate documents. Refer to WPCA's Intranet.
Policy Owner	The WPCA Board and the CEO are the policy's owner and are responsible for oversight of the policy. The policy owners also play a role in approving the policy.
Policy Reviewer	The functional Executive responsible for WPCA Cyber Security and who supports the Policy Owner.
All Senior Executives	Identify policy gaps and participate in policy consultation processes:
Audit & Risk Committee	Meets quarterly to consider and endorse risk and governance-related WPCA Policies and other corporate documents.

This section must be referenced in conjunction with the WPCA Cyber Roles and Responsibilities document.

3.3. Access Control

Business requirements for access control are defined and documented, and access to system components and sensitive information (e.g. WPCA Data) are restricted to only those individuals whose job requires such access. All personnel provided access is given a clear statement of the business requirements to be met by access controls.

- Every user has a single unique user ID and a password to access the WPCA system. Shared, generic or group user IDs and passwords must not be created or used.
- Assignment of privileges must always be based on each individual's job classification and function.
- Level of privilege required for each role (for example, user, administrator, etc.) for accessing resources must be defined.
- Access to privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities.

- Documented approval by authorised parties is required (in writing or electronically) for all access, and it must specify necessary privileges.
- Access controls must be implemented via an automated access control system.
- Access control roles, e.g. access request, access authorisation, and access administration, must be segregated.
- Authentication, authorisation and access controls systems must follow WPCA Access Control Standard.

This section must be referenced in conjunction with the WPCA Access Control Standard.

3.4. Cryptography

To ensure the effective use of cryptography to protect information confidentiality, authenticity, and/or integrity WPCA has developed and implemented a cryptography standard on the use of cryptographic controls for the protection of information.

Making a decision as to whether a cryptographic solution is appropriate is part of the wider process of risk assessment and selection of controls. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control must be applied and for what purpose and operational process.

Specialist advice is sought to identify the appropriate level of protection and to define suitable specifications that will provide the required protection and support for the implementation of a secure key management system.

This section must be referenced in conjunction with the WPCA Cryptography Standard.

3.5. Business Continuity and Disaster Recovery

Information security continuity is embedded in WPCA's business continuity and disaster recovery management systems. There is a managed process in place for developing and maintaining business continuity and disaster recovery throughout WPCA. A strategy plan based on a risk assessment is developed for the overall approach to business continuity and disaster recovery. The strategic plan is dependent on a Threat and Risk Assessment and the Business Impact Analysis (BIA).

3.6. Incident management

To detail clear definitions of the types of incidents that are likely to be encountered and document a plan for corrective action, WPCA has:

- Developed a consistent and effective approach that can be applied to the management of security incidents.
- Established an incident management responsibilities and plan to ensure a quick, effective and orderly response to security incidents and software malfunctions.

- Notified the individuals responsible for handling information security incidents and provided accelerated problem notification, damage control, and problem correction services in the event of computer-related emergencies such as virus outbreaks and hacker break-ins.
- Identified the individuals responsible for handling information systems security incidents and provided them with the authority to handle incidents and create security incident reports.

This section must be referenced in conjunction with the WPCA Incident Response Standard and Plan.

3.7. Information Classification

WPCA information is important and often sensitive. Hence, information must be labelled correctly so that the staff and users within WPCA and NSW Government know how to manage it appropriately, securely, and consistent with the Australian Government and other states and territories.

- Classifications and associated protective controls for information must be suited to business needs for sharing or restricting information and the business impacts associated with such needs.
- Classifications and labelling standards have been developed, implemented and communicated to all staff. The information is classified in terms of its value, legal requirements, sensitivity and criticality to WPCA.

This section must be referenced in conjunction with the WPCA Information Classification Procedure.

3.8. Legal, Regulation and Compliance

WPCA has identified the legislation and regulations it must administer or with which it must comply by implementing this Cyber Security Policy and related Standards.

Areas of risk associated with non-compliance should be identified, analysed, and evaluated, and the details have been recorded as items in the Cyber Security Risk Register. The Register assigns accountability for each item to Risk Owners and Risk Custodians within WPCA.

Risk ratings are assigned to each item, and mitigation strategies have been developed, consistent with WPCA's risk assessment processes.

This section must be referenced in conjunction with the WPCA Legal, Regulation and Compliance Standard.

3.9. Logging and Monitoring

WPCA is committed to defining requirements for accountability and controls for technology logging and monitoring. Detecting potential or actual information security incidents relies on timely and comprehensive event information from crucial security controls. These events are critical during forensic investigation in the event of a security incident. The implementation of technology logging and monitoring improves the detection of malicious behaviour and assists to mitigate information security risks.

WPCA collects and logs data relating to activity and security events on the network, computers, and storage devices, including IT systems and applications. The type of events recorded must be defined based on the system's capability to produce log data and classified information stored within the system as per the WPCA's Information Classification Standard.

Access to WPCA's network, systems and communications is logged and monitored to identify potential misuse of systems or information. Logging activities include regular monitoring of system access to prevent attempts at unauthorised access and confirm access control systems are effective. Log servers should be secured and only made available to the authorised individuals. These logs should be retained as long as necessary or required for practical use or as per state regulation or law.

This section must be referenced in conjunction with the WPCA Logging and Monitoring Standard.

3.10. Media and Equipment management, Sanitisation and Disposal

WPCA produces, receives, uses and manages information and data on behalf of the NSW public, other agencies, states and territories and the Australian Government. This information is important and often sensitive. This policy applies to equipment and media that produce, store, and process information with Dissemination Limiting Marker (DLM) OFFICIAL and above. Please refer to the WPCA'S Information Classification Standard for more details on information classification.

Various technologies are used to store, process, and produce such information and must be handled in a way that appropriately maintains the security of any information that remains on them at the point of disposal. Since technology can process, store or communicate sensitive or classified information, technology equipment and media management, sanitisation, and disposal standards must be in place to outline the requirements to effectively remove information or data owned and/or managed by WPCA.

This section must be referenced in conjunction with the WPCA Media and Equipment management, Sanitisation and Disposal Standard.

3.11. Mobile Device Usage

- A Standard and supporting security measures is in place to manage the risks introduced by mobile devices (such as tablets and smartphones).
- Appropriate controls are implemented to protect against the risks of working with mobile computing facilities, in particular in unprotected environments.
- Tablets and smartphones must not be used for WPCA business information unless configured with the necessary controls and approval for such use.
- Only mobile devices purchased, maintained and/or configured for use by WPCA will be permitted to store WPCA information or permitted to interface with WPCA computers and networks.
- All mobile devices, phones, tablets, and other transportable equipment containing sensitive information must employ storage encryption for all files.

This section must be referenced in conjunction with the WPCA Mobile Device Usage Standard and Acceptable Use Policy.

3.12. Network Security

WPCA is committed to defining requirements for the secure design and management of network infrastructure. Securing the network infrastructure is crucial in providing a reliable operational environment for the NSW administrative and legislative functions. This policy aims to ensure its shared service provider GovConnect, establishes appropriate network security controls to protect WPCA's

technology services and systems against downtime due to malicious and unintentional failures, prevent unauthorised individuals from accessing network resources, and protect confidential data.

This section must be referenced in conjunction with the WPCA Network Security Standard.

3.13. Secure System development

Principles for engineering secure systems have been established by the Authority's shared service provider, GovConnect. In addition to establishing the principles, this includes documenting, maintaining and applying to any information system implementation efforts. WPCA will ensure GovConnect:

- Establishes and appropriately protects secure development environments for system development and integration efforts that cover the entire system development lifecycle.
- Tests security functionality integration into the development process.
- Establishes acceptance criteria for new information systems, upgrades, and new versions must be established, and suitable tests of the system carried out prior to acceptance. Requirements and criteria for acceptance for new systems is to be clearly defined, agreed upon, documented and tested.

This section must be referenced in conjunction with the WPCA Secure System Development Standard.

3.14. Supplier Security

WPCA is committed to and is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its technology systems and applications is secure and protected from cyber adversaries.

The WPCA uses Technology Service providers or third parties to deliver various business services to the organisation. The risks associated with these third parties' use need to be managed so that the WPCA can gain assurance that its information, services, and stakeholders are protected within the WPCA's risk appetite.

WPCA must:

- Agree and document with the supplier on Information security requirements for mitigating the risks associated with the supplier's access to WPCA's assets
- Identify and mandate information security controls to specifically address supplier access to the organisation's information in a policy. These controls should address processes and procedures to be implemented by the organisation, as well as those processes and procedures that the organisation should require the supplier to implement
- Establish and agree on all relevant information security requirements with each supplier that may access, process, store, communicate, or provide IT infrastructure components for WPCA's information.
- Include in agreements with suppliers the requirements to address the information security risks associated with information and communications technology services and product supply chain.

This section must be referenced in conjunction with the WPCA Supplier Security Standard.

3.15. System Hardening

WPCA is committed to defining requirements for securely hardening WPCA technology and applications. Application of this Policy ensures that WPCA technology and applications are appropriately configured and maintained, which reduces WPCA's risk from unauthorised access or data breach of its information assets. Below (including but not limited to) are practices that are followed to ensure the optimum level of security of the systems:

- System hardening standards are developed and implemented;
- Default operating system accounts are disabled, renamed or have their passphrase changed;
- A range of security solutions such as application whitelisting, enhanced mitigation experience toolkit and exploit protection, host-based intrusion prevention system, software firewall, antivirus software and endpoint device control software is implemented; and
- Users do not have the ability to install, uninstall or disable the security system, software or appliances.

This section must be referenced in conjunction with the WPCA System Hardening Standard.

3.16. Vulnerability and Patch Management

WPCA provides a common set of methodologies and requirements to standardise vulnerability scans and patch management across technologies. This Policy ensures technologies are configured and maintained consistently and securely, vulnerabilities are detected, analysed and remediated in a timely manner and patches (including hotfixes, service packs, updates, fixes, and vendor-recommended workarounds) are obtained, tested, and applied in a controlled manner. Furthermore:

- A system is in place for the timely gathering of information about technical vulnerabilities of information systems.
- A Standard has been established to identify new security vulnerabilities, using reputable outside sources for security vulnerability information, and a risk ranking (for example, as "high," "medium," or "low") is assigned to newly discovered security vulnerabilities.
- WPCA's exposure to these vulnerabilities is evaluated by GovConnect, and appropriate measures are taken to address the associated risk across the organisation.
- All patches and security updates are to be pushed out in a formalised and secure manner, with all critical patches installed from a vendor or other approved third party. Installation of all applicable vendor-supplied security patches are applied within an appropriate time frame.

This section must be referenced in conjunction with the WPCA Vulnerability and Patch Management Standard.

3.17. Physical and Personal Security

WPCA must detail the physical security requirements such as computer room requirements, guarding, physical locks, and the security structure of all relevant premises within offices. Furthermore:

- WPCA must use an appropriate security perimeter to protect areas that contain information processing facilities.

- Perimeter security (barriers such as walls, card-controlled entry gates or manned reception desks) must be constructed based on the level of physical security required to protect the WPCA assets contained within all offices.
- If there is an alternate or backup site or off-site storage facility, then the location's security must be reviewed at least annually.
- Secure areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.
- Video cameras and/or access control mechanisms must monitor individual physical access to sensitive areas.
- Secure areas must be created to protect offices, rooms and facilities that are assessed as having special security requirements.
- All staff must ensure doors to sensitive areas, rooms and information processing facilities are locked to prevent unauthorised access when not in use.
- Information systems must be housed in a secure manner to be protected from external and environmental threats such as theft, damage, destruction, flood, fire, etc., to the business premises.
- Computer rooms must have fire detection and suppression, power conditioning, air conditioning, humidity control, and other computing environment protection.

4. Supporting information and resources

- Acceptable Use Policy
- Access Control Standard
- Cryptography Standard
- Cyber Roles and Responsibilities
- Disaster Recovery Standard
- Disaster Recovery Plan
- Incident Response Standard
- Incident Response Plan
- Information Classification Standard
- Legal, Regulation and Compliance Standard
- Logging and Monitoring Standard
- Media and Equipment management, Sanitisation and Disposal Standard
- Mobile Device Usage Standard
- Network Security Standard
- Secure System development Standard
- Supplier Security Standard
- System Hardening Standard
- Vulnerability and Patch Management Standard
- Physical and Personal Security Standard

Western Parkland City Authority

Level 2, 10 Valentine Avenue
Parramatta NSW 2150

T: 1800 312 999
E: hello@wpca.sydney
W: wpca.sydney

NSW GOVERNMENT