Table of Contents

[Table of Contents 1](#_Toc115246365)

[1. Underlying Principles 2](#_Toc115246366)

[2. Background and Purpose 2](#_Toc115246367)

[3. Scope and Intent 3](#_Toc115246368)

[4. Applicability and Responsibility 3](#_Toc115246369)

[4.1. Breaches of Policy 4](#_Toc115246370)

[5. Policy 4](#_Toc115246371)

[5.1. General Principles 4](#_Toc115246372)

[5.1.1. Risk appetite and tolerance 4](#_Toc115246373)

[5.2. Access Authorisation 5](#_Toc115246374)

[5.2.1. Information Asset Stewards and Information System Administrators 5](#_Toc115246375)

[5.3. Account Management 6](#_Toc115246376)

[5.3.1. Account Management 6](#_Toc115246377)

[5.3.2. Account Revocation 8](#_Toc115246378)

[5.3.3. Privleged Account Management 9](#_Toc115246379)

[5.4. Authentication 9](#_Toc115246380)

[5.5. Offline Information Assets 9](#_Toc115246381)

[5.5.1. Offline assets 9](#_Toc115246382)

[5.5.2. Requesting an extract 10](#_Toc115246383)

[5.5.3. Access assignment 10](#_Toc115246384)

[5.5.4. Intellectual property rights 10](#_Toc115246385)

[5.5.5. Expiry of information asset extract 11](#_Toc115246386)

[5.6. Access Monitoring and Reporting 11](#_Toc115246387)

[6. Definitions 11](#_Toc115246388)

[7. Governance 11](#_Toc115246389)

[8. Document version history 12](#_Toc115246390)

[9. Appendix One: Access Request Workflow 13](#_Toc115246391)

[10. Appendix Two: References 14](#_Toc115246392)

# Underlying Principles

A number of underlying principles underpins this policy. These principles are:

* Wannon Water creates, consumes, and holds significant amounts of raw data, from which significant information assets can be derived and identified
* These information assets are consumed, generated and manipulated in a number of information systems owned and operated by Wannon Water
* Wannon Water recognises value in our information assets and systems
* There is interest in the consumption of our information assets by external agencies
* Wannon Water is committed to protecting the Integrity, Availability and Confidentiality of our valued Information Assets
* Wannon Water accepts the concept of least privilege as a core control to ensure the Integrity, Availability and Confidentiality of our information assets, and we accept access control as a primary control to do this.

# Background and Purpose

This policy forms a component of Wannon Water’s Cyber Resilience Strategy and is designed to provide a working framework within which to govern the provision of consumer and management access to Wannon Water’s information assets.

It will cover:

* Provision of access
* Maintenance of access, including changes to access or access levels
* Revocation of access including voluntary or automatic rights repudiation
* Privileges and accountability determination mechanisms
* Authentication and Identity mechanisms to the extent they relate to access to Wannon Water’s information assets.

Note that the intent of this policy is also to govern access to any subset or extract of or from any Wannon Water information asset.

This document will present guidance in line with relevant Victorian and Australian Government standards including:

* The Victorian Protective Data Security Framework (VPDSF)
* The Federal Protective Security Policy Framework, specifically INFOSEC 9 – Access to Information
* Australian Signals Directorate Information Security Manual.

Where relevant, guidance shall also be presented from other Government standards and industry best practice guides such as:

* Statement of Direction for the Victorian Public Service: Workforce and Access Management
* National Institute of Standards and Technology Cyber Security Framework (NIST CSF)
* National Institute of Standards and Technology Special Publication 800-53 (r4) (NIST 800-53), in particular the Access Control (AC) control family[[1]](#footnote-2)
* National Institute of Standards and Technology Special Publication 800-82 (NIST 800-82)
* The Information Technology Infrastructure Library (ITIL) framework
* The Control Objectives for Information and Related Technologies (COBIT) framework.

As part of the Cyber Resilience Strategy, Wannon Water has elected to align its cyber control framework to NIST 800-53 (r4), NIST 800-53 (r4) controls and general terminology will be referenced throughout this document.

# Scope and Intent

This policy will apply to the management of access of or to any Wannon Water information asset either in its entirety or any part of in any form, including offline extracts.

This includes all information assets identified in the Wannon Water Information Assets Register, and any other information assets not as yet identified that could reasonably be considered an Information Asset. The intent behind this will be understood to include the following constituting components of these information assets:

* Any raw DATA in any format
* Any software or software system used to:
  + Create any component of the asset
  + Store or manage holding of the asset or a component of the asset
  + Manipulate, calculate, modify, document or report on the asset
  + Report on or present the asset for consumption
* Any extract of information (or raw data) from the asset, including in hardcopy.

Note that it is explicitly intended to include access controls to any extracts of any information asset within the scope of this policy. The intent of this inclusion is to ensure consistency between access management of information assets and subset and extracts of those assets.

While not intended as a technical document, certain technical terminology and principles will be used as appropriate throughout this document.

# Applicability and Responsibility

This policy will be applied to all requests for access to Wannon Water’s information assets. In practice, this means the policy will apply to:

* All Wannon Water employees
* All Wannon Water contractors, their employees and agents. This includes contractors employed under fixed contracts, operational agreements and ad hoc arrangements
* Customers
* Vendors and suppliers
* Government agencies and regulators.

Responsibility for the governance and ongoing maintenance of this policy is as follows:

|  |  |  |
| --- | --- | --- |
| Accountability | Role | Person/Body |
| Responsible | Maintenance of policy | * Information Security Manager * Cyber Resilience Working Group |
| Application of policy guidelines | * Digital Services Team * Information Stewards * Information Systems Administrators |
| Accountable | Ownership of policy | * Chief Information Officer |
| Consulted | Input into policy guidelines | * Digital Services Team * OT team * Information Governance Committee * Enterprise Architecture Committee |
| Informed | Informed of policy | * All Wannon Water staff * External consumers of Wannon Water information assets |

*Figure 1: Responsibility and Accountability*

## Breaches of Policy

Breaches of this policy will be treated as a Cyber Incident and be investigated under the guidelines of the ***Wannon Water Cyber Incident Response Framework***.

Willful or negligent breaches of this policy may result in Wannon Water team member being sanctioned under ***Wannon Water’s Consequence of Employee Misconduct*** process, at the discretion of the Chief Information Officer.

It should be noted that breaches of this procedure may result in a contravention of the Victorian Protective Data Security Standards, or other relevant regulations or legislation and may result in notification to a regulatory body such as DPC or OVIC. In such cases external penalties may apply.

# Policy

## General Principles

This policy will adhere to these general principles of access management.

### Risk appetite and tolerance

Wannon Water’s information assets are critical to its operations - reliable information leads to reliable business decisions, with corresponding efficiency and customer satisfaction gains. Wannon Water has an obligation to ensure the integrity, availability and confidentiality of information assets. A key control in ensuring the veracity of our information assets are access controls.

The principle of least access, a widely adopted cyber control, states that users and consumers of information should only have sufficient access to ensure their role. This principle is effectively controlled by access control rules and guidelines, and will be adopted as a core principle by this policy.

Key to assessing our access controls is the level of risk we are willing to accept (appetite) and tolerate (tolerance) to the veracity of our information. An organisation’s risk appetite will clearly affect the level and complexity of controls[[2]](#footnote-3).

Wannon Water currently has a low risk appetite and tolerance, so this policy will be detailed accordingly. This policy is designed to support a low risk approach to access control.

## Access Authorisation

All access to a Wannon Water information asset **must** be authorised by the appropriate Authority. This Authority will be an individual delegate with the authority to create, modify and revoke access to a particular information asset as delegated by the owner of that information asset. Typically within Wannon Water, this will be an Information Steward . In some instances, the Authority may also physically grant the access permissions, but in many cases this physical provisioning will be undertaken a designated system administrator , or by the IT team.

No access rights will be granted to any Information Asset or Information System without appropriate authorisation from the relevant Authority.

Note that in certain circumstances, such as during a cyber incident, the IT team, acting on the authority of the Chief Information Officer, the ISIRT, or IMT, may unilaterally provide, modify or revoke access permissions as reasonably required.

### Information Asset Stewards and Information System Administrators

An Information Steward is an officer that has been delegated authority and responsibility for the maintenance of an information asset by that information assets owner. The roles and responsibilities of Stewards are defined in document CD2020/00716 ***Information Management Custodian Model***, and include maintaining the security for their designated asset. Information Stewards will act as access Authorities for the assets they are responsible for.

System administrators are officers who have privileged access to one or more information systems (I.e., applications) that support information Assets. Information Stewards delegate authority to undertake system administration roles to these System Administrators. In some cases Information Stewards may also be System Administrators, but more often than not a single System Administrator may support several Information Assets – take for instance the Finance One system. This information system hosts multiple Information Assets, and therefore has multiple Information Stewards, but being a single digital eco system, it makes sense for it to have one System Administrator.

The System Administrators role can be thought of as the ‘technical expert’, and would typically undertake the following tasks:

* Apply updates and patches, under the guidelines of the Wannon Water Change and Configuration Management Process
* Manage user and access adds, moves and changes
* Provide day to day operational support
* Provide expert advice
* Assist in system development and upgrades
* Maintain the integrity of the information system, including data processing rules and system security.

Typically there will be no more than two Information System Administrators per Information System to limit the use of privileged access accounts, and to place a degree of control over changes. Wherever practical, privileged access (I.e. administrator level access) will be via specialised restricted administrative accounts rather than day to day accounts.

To support the concept of separation of duties, an Information System Administrator must not make any change to the access rights of any user without the authorisation of the relevant Authority. In terms of the RACI model, the relevant roles and authority of Information System Administrators and Information Stewards in terms of access management can be summarised as below in Figure 2:

|  |  |  |
| --- | --- | --- |
| Role | Accountability | Comments |
| Information Steward | Accountable | The Steward is accountable for access control. The Steward will authorise any and all access changes. The Steward must confirm to the best of their ability that the Administrator is effectively applying access controls as authorised by the Steward. |
| Information System Administrator (including IT) | Responsible | The Administrator is responsible for maintaining access control, and will implement any authorised access requests, as authorised by the Steward. The Administrator must verify that any access request has been duly authorised by the appropriatre Authority before implimenting any access change. |

*Figure2: Steward and Administrator roles*

## Account Management

### Account Management

The primary access management agent will be a user account –i.e. a user account will be the agent via which an individual obtains access to an information asset.

This user account may be a global account shared across assets (i.e. an Active Directory) account, or local to a particular system (i.e. an Asana log in).

As a general baseline, accounts will:

* Be unique, and whenever possible linked to a natural person, with the preferred format of <firstname.lastname>
* Be configured as a challenge – response mechanism (i.e. a password)
* Be configured to disable after a defined challenge – response failure repetition (i.e. lockout)
* Be assigned role based privileges
* Be auditable wherever possible
* Be capable of disablement wherever possible
* For temporary accounts (i.e. contractors) be set with pre-defined usage conditions (i.e. time restricted access, asset restricted etc.) with a pre-defined account disable time
* Accounts are disabled after a defined period of inactivity
* Where possible, Active Directory accounts will be used. Active Directory is centrally managed and has significant security management tools built in
* Where possible, privileged access accounts will be separated from day to day access accounts.

Please refer to the ***Password Procedure*** and the ***Information Technology Security Procedure***for further details.

#### Account Creation Process

The creation of all accounts must be requested by the appropriate authorising Authority. This Authority will be a Wannon Water officer with appropriate authority to permit or modify access to a Wannon Water information asset, as delegated by the ‘Owner’ of that asset. Typically this will be a designated Information Steward, or Information System Administrator.

Typically, accounts will be created by Wannon Waters’ IT Team, although in some instances discrete system accounts will be created by an Information Asset Steward.

Accounts (other than emergency accounts) will only be created on receipt of a request from an authorised authority.

#### Temporary Accounts

Temporary accounts will be created for time limited engagements (i.e. contractors or fixed term employment). As with standard accounts, all temporary accounts must be authorised by the appropriate Authority. Any temporary accounts will be created with the following attributes:

* Minimal access privileges designed to achieve the required works
* Appropriate asset or time based access controls, as appropriate. For instance an account may be created for a contractor allowing only access to a specific asset during specified hours of the day, connecting from a specified location
* Be regularly audited
* Be identifiable as a temporary account (i.e. metadata labelled, created in a special system container for temporary accounts)
* Be automatically time expired where possible. For instance a contractor’s account may be set to automatically disable on the due date of completion of their engagement.

#### Emergency Accounts

From time to time it may become necessary to create emergency accounts in a system. Emergency accounts will typically have a significantly higher level of access privileges than standard accounts and are typically required urgently, in response to an exigent circumstance. In such instances, the standard account and access enablement processes may be inappropriate.

Emergency accounts are not intended for permanent use and are considered to be very short term in duration, created to assist resolution of a specific issue.

An emergency account must be authorised by one of the following officers:

* The Chief Information Officer
* The IT Operations Manager
* The Manager Electrical and Mechanical Services
* The ISIRT
* The Incident Controller of a duly formed IMT
* Information Security Manager.

An emergency account must only be created during exigent circumstances where it is obvious the standard account creation process is inappropriate or can’t be followed.

All emergency accounts must be disabled on resolution of the circumstances that caused their creation.

### Account Revocation

All accounts will be suspended on notification from the appropriate Authority of a request to suspend an account. Accounts can be either temporarily suspended, or permanently suspended.

#### Temporary Suspension

An account may be temporarily suspended when an account principle (I.e. the ‘holder’ of the account) is unable to ‘access’ the account for an extended period of time, for instance on extended medical leave, or a contractor ending their period of engagement but with an expectation of being awarded further works in future.

Note that a suspended account does not have its access rights revoked, but merely suspended – on reactivation, the account retains all of its pre- suspension access rights.

Note that in certain circumstances, the suspension of an account may not be appropriate – for instance a team member going on extended long service leave who still requires access to email. Suspending their account will disable this access completely, so in these cases it is more appropriate to revoke access rights to all but the minimum information assets needed under these circumstances.

#### Permanent Suspension

There will be circumstances where an account needs to be permanently suspended or disabled, examples of such may be a team member leaving Wannon Water, a contractor completing their engagement with no immediate further engagement planned. In most circumstances it may not be desirable to immediately revoke (i.e. delete) that account, but to disable it with no intention of reactivation under normal operating circumstances.

Accounts permanently suspended will be reviewed every six (6) months through the Authorised Access Review process (refer to ref CD2020/00718) and if no longer required, revoked (i.e. deleted or archived).

#### Emergency Revocation

Accounts (and access) may be revoked by the IT team in an ‘emergency’ situation without consultation if required and as directed by the:

* Chief Information Officer
* Information Security Manager
* Information Technology Operations Manager
* Information Security Incident Response Team
* Incident Response Team
* Notification from either Victorian Government Cyber Security Unit, DEWLP or OVIC.

Typically an ‘emergency’ situation would be:

* An active cyber incident within Wannon Water
* An active cyber incident impacting a supplier or contractor
* An active cyber incident impacting Australian or Victorian government
* Suspicious account activity leading rise to concerns of compromise.

Access suspended during such an ‘emergency’ event will in general be restored at the conclusion of the ‘emergency’ event, following the appropriate investigation.

### Privleged Account Management

Wherever possible privileged accounts, that is, accounts with a level of administrative privilege, will be separate to day to day accounts.

All privileged accounts will be wherever technically possible, secured by MFA.

## Authentication

All access accounts will enforce authentication. That is, the access account itself will enforce some form of challenge – response authentication to confirm the veracity of the access account credentials. This authentication will comprise an encrypted password and where possible, a form of multi factor authentication.

Wherever possible, information systems will employ Active Directory authentication and MFA, particularly where the application is:

a) Public facing

b) SaaS or public cloud based

c) Stores or manipulates information assets of a statewide significance[[3]](#footnote-4).

Where information systems cannot use the above authentication methods, other methods must be used – all information systems must authenticate securely with encrypted passwords or tokens. Note that storage or transfer of unencrypted plain text authentication tokens is **not** acceptable – all authentication must be encrypted to an acceptable standard. Please refer to ACSC guidelines such as the ***Information Security Manual*** for current government encryption requirements.

## Offline Information Assets

### Offline assets

It is common to produce one off or regular extracts or subsets of information from existing Wannon Water information assets and share these with stakeholders and consumers. Such extracts typically take the form of reports or data sets, and can take the form of static electronic or hardcopy artifacts.

Such ‘offline’ reports or extracts are still Wannon Water information assets, and as such still require active access management control over their lifetimes. This includes information extracts that are provided to third parties, although note that this **may** exclude certain pieces of personally identifying information where there may be transferable ownership rights provided to the recipient, depending upon relevant legislation (i.e. PII rights under the EU General Protection Regulation or other equivalent provisions)[[4]](#footnote-5).

### Requesting an extract

All extracts of information from an information asset must be approved by the appropriate Authority, typically the information asset steward.

All requests for extracts (including custom reports) must be submitted to the Information Steward via Wannon Waters’ “Request for Data” e-form (<https://eforms-prod.wannonwater.com.au/produce/wizard/161f3a89-3660-4c78-8a4a-1321637ada0e/>)

This e-form will then comprise a record of the request, authorisation and creation of the extract.

Any request for extraction of information from any other information asset not listed on the e-form must be submitted via email to the Chief Information Officer for approval.

### Access assignment

Assignment of access rights to an information asset extract is the responsibility of the Information Steward. The steward is responsible for maintaining the confidentiality, integrity and accessibility of their information asset, including any extracts or reports created and / or shared from it.

The Information Steward is responsible for ensuring appropriate access rights to information asset extracts both initially, as part of the initial creation of the extract or report, and ongoing, for the life of the extract. In effect, the Information Steward must take all reasonable steps to ensure appropriate access controls are maintained on the information asset extract for the duration of its existence, including those extracts provided to third parties.

The Information Steward must make all reasonable effort to ensure any third party the information asset extract is provided to has adequate information security controls to protect the information asset extract to the extent Wannon Water requires it protected.

### Intellectual property rights

Unless otherwise stated in any contract, agreement or legislative or regulatory requirement, Wannon Water retains the rights to any intellectual property created in the process of producing or providing any extract, report or statement from a Wannon Water information asset. Wannon Water may assign the right to access and use that intellectual property to any recipient, but will retain full rights at all times.

Wannon Water will follow the guidelines outlined in the ***Intellectual Property Guidelines for the Victorian Public Sector (2015)*** and the ***Whole of Victorian Government Intellectual Property Policy (2012).***

### Expiry of information asset extract

Typically any information asset extract will have a fixed life, as they are static, point in time extracts from a dynamic asset. That being the case, a static extract still has value (for instance in a historic trend model) and should still be access managed.

It is the responsibility of the Information Steward to ensure:

* The end of life date is understood by all consumers of the information asset extract
* All time expired information asset extracts are removed from general use. This includes those sent to third parties (this may involve confirmation from the third party that the information asset extract has been destroyed )
* As time expired information asset extracts typically still have some historic value, they assign appropriate access controls to those extracts.

## Access Monitoring and Reporting

Access privileges will be reviewed every six months. Please refer to ***the Information System Authorised Access Six Monthly Review*** procedure for more information.

It is the responsibility of individual Information Stewards / Information System Administrators to undertake access reviews, and the accountability of Information Asset / Information Systems owners to ensure such reviews are completed in a timely fashion. The Information Security Manager has oversight of this review and works with the appropriate Information Stewards / Information System Administrators to ensure its completion.

# Defini**tions**

|  |  |
| --- | --- |
| Term | Means |
| IMT | Incident Management Team |
| ISIRT | Information Security Incident Response Team |
| SaaS | Software as a Service |

# Governance

|  |  |
| --- | --- |
| **Associated procedures/standards** | NIL |
| **Legislation and standards** | Victorian Protective Data Security Standards , ACSC Essential 8 |
| **Category** | Non–IMS |
| **Endorsement** | Chief Information Officer |
| **Approval** | Chief Information Officer |
| **Policy owner** | Chief Information Officer |
| **Content enquiries** | Information Security Manager |

# Document version history

|  |  |
| --- | --- |
| Version | Changes made to document |
| 1 | Original document |
| 2 | Updated to the new SoControl template |

# Appendix One: Access Request Workflow

Diagram

Description automatically generated

# Appendix Two: References

Australian Cyber Security Centre, Australian Government Information Security Manual, Commonwealth of Australia, Canberra ACT, 2018

Commonwealth of Australia, Protective Security Policy Framework: Infosec 9 Access to information, Commonwealth of Australia, Canberra ACT, 2019

Commonwealth of Australia, Protective Security Policy Framework: Infosec 10 Safeguarding information from cyber threats, Commonwealth of Australia, Canberra ACT, 2019

Department of Treasury and Finance, Intellectual Property Guidelines for the Victorian Public Sector, version 1.1, State of Victoria, Melbourne Victoria, 2019

Department of Treasury and Finance, Intellectual Property Policy, State of Victoria, Melbourne, 2012

ISACA COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, ISACA, Rolling Meadows Illinois, 2012

ISACA, The Risk IT Framework, ISACA, Rolling Meadows Illinois, 2009

National Institute of Standards and Technology, NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organisations, Revision 4, United States Department of Commerce, Washington DC, 2013

Office of the Victorian Information Commissioner, Victorian Protective Data Security Framework, State of Victoria, Melbourne Victoria, 2018

Raschke, J. and Walsh, K *Sustainable Development for Digital Transformation, Part 1: Applying Environmental Theory to the Digital Ecosystem*, ISACA Journal, Volume 5 2019, ISACA, Schaumburg Illinois, 2019

Souffer, K, Pillitteris, V, Lightman, S, Abrams, M, Hahn, A, NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security, Revision 2, United States Department of Commerce, Washington DC, 2015

1. This control family can be found in detail in NIST SP 800-53 Appendix F [↑](#footnote-ref-2)
2. NIST 800-53 control AC-1 guidance, 2018 [↑](#footnote-ref-3)
3. Defined by OVIC as of BIL level 3 or higher. Refer to [www.ovic.gov.au](http://www.ovic.gov.au) for more information [↑](#footnote-ref-4)
4. Information provided to a third party may have a degree of novation to it – that is, that information is used by the third party to derive a ‘new’ piece of information that although directly related to the source, is not owned by Wannon Water. While the original information belongs to Wannon Water, the ‘newly created’ piece of information does not. [↑](#footnote-ref-5)