# Purpose

This policy is designed to ensure the protection of the corporation's physical assets and the safety of its employees, contractors, and visitors.

# Scope

This policy applies to all employees.

This policy applies to all facilities and locations owned or leased by the corporation and includes co-hosted sites where Wannon Water equipment is located on third party premises.

# Policy statement

Wannon Water shall implement the following physical security measures to safeguard its assets and personnel:

**Access Control** Access to the corporation's facilities shall be controlled and where possible monitored to prevent unauthorised access. Access control measures include:

* Physical barriers, such as fences and gates as defined in the Site Security Standards,
* Where assets are mounted inside cabinets or enclosures, these cabinets or enclosures be security rated
* Security coded locks and padlocks on all doors, gates and fences
* Electronic access control systems

All visitors shall be required to sign in and out of the facility, and will be supervised by an authorised employee or contractor.

Access will be granted acording to the principles of Least Access and Zero Trust. Access to sensitive areas, such as control rooms and data centers, shall be restricted to authorised personnel only.

**Remote Assets:** Where a Wannon Water asset or assets are contained remotely within a third party’s asset, that Wannon Water asset must be secured against unuathorised access. This will at a minimum include a security rated cabinet and lock. Appropriate intrusion detection alarming will be fitted wherever possible.

**Security Cameras:** The corporation shall install and maintain a video surveillance system to monitor all entry and exit points, as well as other critical areas. All recorded footage shall be stored securely. Access to recorded footage will be by authorised officers only, with all access being logged.

Note that Security Cameras are considered a passive security control and will only be used in addition to appropriate access controls.

**Alarm Systems:** The corporation shall install and maintain intrustion detection systems to detect any unauthorised access or intrusion into its facilities. These systems shall be monitored by authorised personel or contractors.

**Lighting:** All facilities and their surroundings shall be adequately lit to deter intruders and enhance visibility and safety of personell during night time operations Security lighting where fitted will comply with relevant Australian Standards such as AS2293:1:2018 and the Australian Government [*Protective Security Policy Framework Policy 16: Entity Facilities*](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.protectivesecurity.gov.au%2Fsites%2Fdefault%2Ffiles%2F2020-04%2FPolicy16-Entity_facilities-8July2019.DOCX&wdOrigin=BROWSELINK)*.*

**Key / Electronic Token Control:** Keys and electronic tokens to the corporation's facilities shall be issued only to authorised personnel, and their distribution shall be documented and monitored. Keys shall be returned when no longer needed or when an employee or contractor leaves the corporation. Electronic tokens will be immediately disabled and then returned when access is no longer required.

Lost keys or tokens will be reported immediately.

Following the concepts of least access and zero trust, keys and tokens with the least access level required by personell or contractors will be issued – that is, master keys will not be issued.

Keys or tokens issued to contractors will be counter authorised by an appropriate officer authorising the works requiring access.

Electronic tokens issued to contractors will be pre-programmed to expire at the end of an authorised period of access.

**Personnel Training:** All employees, contractors, and visitors shall be trained in the corporation's physical security policies and procedures. This includes how to respond to emergencies, how to report suspicious activities, and how to use access control systems.

**Contractor Management:** The corporation shall ensure that all contractors hired to perform work on its facilities comply with its physical security policies and procedures. All contractors will be managed via Wannon Waters Contractor Management System.

**Physical Security Risk Assessment:** The corporation shall conduct periodic physical security risk assessments to identify vulnerabilities and implement appropriate measures to mitigate the identified risks.

**Patrol and Site Monitoring**: The authority will routinely patrol and monitor physical security systems for sites deemed necessary. This may take the form of formal security patrols, routine site visits by officers, or remote monitoring via electronic systems.

**Breach of Policy:** Any detected breach of policy will be recorded as an incident in the Authority’s risk and incident management system. Breaches will be investigated following standard Wannon Water practices. Where appropriate, breaches will be reported to appropriate authorities.

This policy shall be reviewed and updated periodically to ensure its effectiveness. The corporation shall continuously strive to enhance its physical security measures to protect its assets and personnel

# Defini**tions**

|  |  |
| --- | --- |
| Term | Means |
| Electronic token | An electronic device that works as a ‘pass key’ for an electronic locking system. An example of an eletronic token is a Cardax card. |
| Least Access and Zero trust | Security concepts where only the lowest level of access required to perform a task is provided |
|  |  |

# Governance

|  |  |
| --- | --- |
| **Associated procedures/standards** |  |
| **Legislation and standards** | Australian Protective Security Policy Framework Standard 16: Entitiy Facilities |
| **Endorsement** | IT and OT Governance Committee |
| **Approval** | Chief Information Officer |
| **Policy owner** | Chief Inforamation Officer |
| **Content enquiries** | Digital Platform Manager |

# Document version history

|  |  |
| --- | --- |
| Version | Changes made to document |
| 1 | New document |
|  |  |
|  |  |
|  |  |