

PROCESS, INSTRUMENTATION AND CONTROLS

ORGANISATIONAL PHYSICAL SECURITY STANDARD

Document No. ESF-500-STD-406

Copyright information

Copyright © Watercare Services Limited. All rights reserved.

Disclaimer

Watercare Services Limited has endeavoured to ensure material in this document is technically accurate and reflects legal requirements. However, the document does not override governing legislation.

Watercare Services Limited does not accept liability for any consequences arising from the use of this document. If the user of this document is unsure whether the material is correct, they should refer directly to the relevant legislation and contact Watercare Services Limited.

More information

If you have further queries, please contact the **Security team** at: securityteam@water.co.nz

DOCUMENT CONTROL

Document owner

Role Security Manager

Organisation Watercare Services Limited

Version history

Version	Description of revision	Published By	Date
1.0	First release	Waldo Strydom	19/2/2024

Approvers / Reviewers

Name	Title	Role
Chris Philp	Security Consultant	Author
Waldo Strydom	Principal Asset Lifecycle Engineer	Reviewer
Alan Foubister	Security Manager	Reviewer / Approver

Table of contents

DOCUMENT CONTROL.....	3
DOCUMENT OWNER.....	3
VERSION HISTORY.....	3
APPROVERS / REVIEWERS.....	3
TABLE OF CONTENTS	4
1. INTRODUCTION	6
2. METHODOLOGY	7
2.1 REVIEW.....	7
2.2 THREAT AND RISK	7
2.3 DETER, DETECT, DELAY, RESPOND	11
2.4 CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED)	11
2.5 SECURITY IN DEPTH	12
2.6 PSR SECURITY ZONES.....	12
2.7 PHYSICAL SECURITY LIFECYCLE.....	14
3. SITE SPECIFIC SECURITY CONTROLS.....	15
3.1 SITE-SPECIFIC RISK ASSESSMENT	15
3.2 PHYSICAL SECURITY MEASURES REQUIRED.	15
4. PHYSICAL SECURITY STANDARDS.....	17
4.1 SPECIFIC LANGUAGE FOR COMPLIANCE	17
4.2 BEYOND THE PERIMETER (PROJECTED SECURITY MEASURES).....	17
4.2.1 <i>Security culture and training</i>	17
4.2.2 <i>Security communication</i>	17
4.2.3 <i>Signage</i>	18
4.3 PERIMETER	19
4.3.1 <i>Perimeter fencing</i>	19
4.3.2 <i>Perimeter access points</i>	21
4.4 SITE (INCLUDING RESERVOIRS).....	24
4.4.1 <i>Site appearance and maintenance</i>	24
4.4.2 <i>Fresh water and wet well doors and hatches</i>	24
4.4.3 <i>Unhoused operational assets</i>	25
4.5 BUILDINGS	25
4.5.1 <i>Reception areas</i>	26
4.5.2 <i>PSR security zones</i>	28
4.6 GENERAL	34
4.6.1 <i>Security lighting</i>	34
4.6.2 <i>CCTV</i>	35
4.6.3 <i>IDS</i>	38
4.6.4 <i>EACS</i>	38
4.6.5 <i>SSP</i>	39
4.6.6 <i>Security communications network</i>	39
4.6.7 <i>Electronic security cabinets</i>	40
4.6.8 <i>Security cabling</i>	40
APPENDIX A – USEFUL REFERENCES	41
APPENDIX B – CURRENT THREAT ASSESSMENT	42
APPENDIX C – BASELINE RISKS	43
APPENDIX D – WATERCARE SPECIFIC BUSINESS IMPACT LEVELS	45

APPENDIX E – GUIDANCE ON SETTING RISK LEVELS	46
APPENDIX F – EXAMPLE ALERT LEVEL SYSTEM	48
APPENDIX G – PUMP STATION BASELINE CONTROLS	50

1. Introduction

Physical security is intended to protect assets to ensure Watercare can continue to supply reliable, high-quality drinking water and wastewater services. Physical security control measures are required for sites and buildings to protect Watercare property, information and people.

Implementation of the requirements contained in this document contains both physical controls, awareness and training for appropriate staff and partners to ensure they correctly understand both purpose and implementation.

This document does not address Cyber Security but applies to staff, contractors and consultants undertaking design, construction, or review of **Physical Security** systems at all sites owned or managed by Watercare.

This document supports the need for a proactive security culture and provides guidance on determining the physical security risk profile, and the minimum standard for physical security control measures to mitigate security risks to an acceptable level. This document should be referenced by project managers and site managers anytime significant works are undertaken on an existing site, or when a new site is being developed.

This document is intended to be comprehensive, however project managers, site managers and other users of this document must consult with the Watercare Security Team to ensure appropriate physical security control measures can be integrated into the project design at the earliest opportunity.

This Standard should be read in conjunction with the following Watercare documents:

- Watercare CCTV Policy
- [Watercare Risk Management Framework](#)
- [Watercare Architectural Guidelines \(DP-12\)](#)
- [Watercare Material Supply Standard](#)

Other relevant and useful legislation, policies and standards are listed in Appendix A.

2. Methodology

This section provides an overview of the methodologies and concepts that are relevant to this standard.

2.1 Review

The Watercare Security Manager will review this standard annually, or whenever there is a significant change in the security environment, to ensure the security controls and standards remain fit for purpose.

Security threats and risks may differ greatly from site to site. Project managers and site managers should review site-specific threat and risk assessments whenever there is a significant change in the security environment, or every three years as a minimum.

2.2 Threat and risk

To ensure appropriate and proportionate physical security measures are implemented, a good understanding of threat and risk is required.

Threat identifies an action or event that leads to a negative outcome, who or what perpetrates that action or event and the likelihood of that action or event occurring. For example, a threat may relate to the potential theft of tools from a storage shed on a site by petty criminals. The likelihood of this occurring will be site specific and may depend on factors such as the local crime rate.

Risk takes into account the impact or consequences that would result from the threat action or event occurring. For example, if the tools were low value and used only for routine maintenance, the impact of them being stolen might be low. However, if the tools were critical in ensuring the operation of the site function and difficult to replace, the impact of them being stolen might be very high.

The relationship between threat and risk is shown in Figure 1.

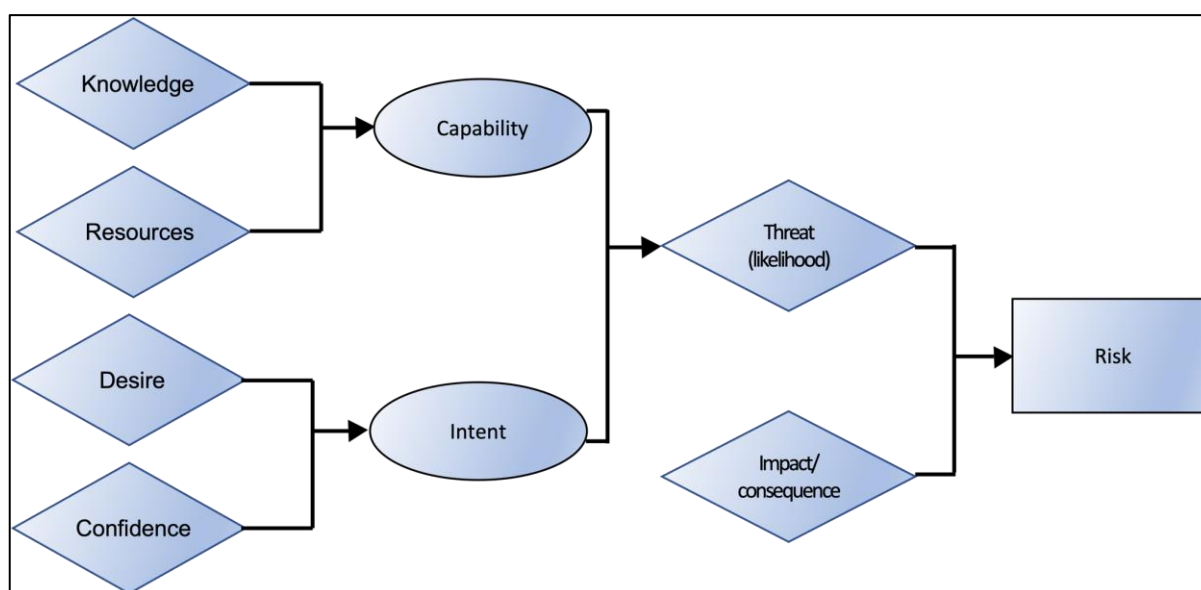


Figure 1 – Threat and risk relationship.

A high-level description of the assessed threat types and actors faced by Watercare, as a lifeline utility provider, are provided in Table 1 below. The current assessed threat levels are contained in Appendix B. It is important to note that threat assessments are a snapshot in time and change as the threat environment changes. Not only do threat levels change, but new threat vectors may develop. Both the threat types and actors, along with the threat levels, should be constantly monitored and reviewed, both at an organisational and site level.

Table 1 – Description of threat type and actors.

THREAT	Actor / description
TERRORISM	A terrorist is someone who is willing to threaten or use violence in pursuit of political or ideological aims. The threat of terrorism can come from both international or domestic individuals or groups, and can include extremists across the spectrum of religious, identify, issues-motivated or other motivations.
DISRUPTIVE ACTIVITY	Protestors, activists or issues-motivated groups are those who campaign to bring about political or social change and are willing to take physical action in support of their cause which may cause disruption to Watercare activities or operations.
	Fixated or Acutely Disaffected Persons (ADP) are individuals who have an obsessional pre-occupation with a person, place or cause which is pursued to an irrational degree, which may cause disruption to Watercare activities or operations.
SABOTAGE / UNAUTHORISED DISCLOSURE OF INFORMATION	An insider is a person who has legitimate access to a Watercare site, who use their legitimate access to target areas they are not authorised to access, use information for unauthorised purposes or cause damage to Watercare assets. Insiders can include staff, contractors and authorised visitors.
	Hostile intelligence activity includes foreign government sponsored and commercial/industrial espionage, targeting Watercare information or assets.
	Investigative journalist and other media outlets may publicly disclose Watercare proprietary information through their publications.
GENERAL CRIME	The threat of violence, theft and vandalism may come from a variety of threat actors, including petty/opportunistic or motivated criminals.
	Organised criminal activity is generally well planned and resourced. It will usually be motivated by financial gain, either directly (e.g. cash or high-value assets) or indirectly (e.g. chemicals useful in the manufacture of illegal drugs).
ECONOMIC CRIME	Cybercrime is any criminal activity that takes places via the internet. Generally this will be conducted by criminal groups motivated by financial gain but could also include actors targeting control or other communications systems aiming to disrupt Watercare activities or operations.

Identifying instances of how these threats could occur and assessing the impact or consequences of this results in a set of risks. Further details on risk assessment can be found in the Watercare Risk Management Framework policy document. The most significant risks faced by Watercare relevant to the physical security of sites are listed in Table 2, with further detail provided in Appendix C. It should be noted that these are general risks across the Watercare portfolio and site-specific risk ratings may vary across different sites.

Table 2 – Matrix of baseline risks

RISK TYPE	Theft							Vandalism				Contamination of fresh water Release of wastewater				Intentional harm	
BUSINESS IMPACT	Financial loss			Reputational damage or disruption to operations		Loss of information		Reputational damage		Disruption to operations		Reputational damage		Detrimental health effects		Harm to staff or other site occupants	
THREAT ACTOR	Petty criminal	Motivated criminal	Insider	Petty criminal	Motivated criminal	Motivated criminal	Insider	Petty criminal	Activist/terrorist	Petty criminal	Activist/terrorist	Petty criminal	Activist/terrorist	Petty criminal	Activist/terrorist	Petty /Motivated Criminals	ADP
Water Treatment Plant	High	Med	Low	Med	Low	Low	Med	High	Low	Med	Med	Med	Med	Low	Low	Low	Med
Wastewater Treatment Plant	High	Med	Low	Med	Low	Low	Med	High	Low	Med	Med	Low	Low	Low	Low	Low	Med
Office Laboratory or	Med	Med	Low	Low	Low	Med	Med	Med	Low	Low	Med	N/A	N/A	N/A	N/A	Low	Med
Maintenance Depot	High	Med	Med	Low	Med	Low	Low	Med	Low	Low	Med	N/A	N/A	N/A	N/A	Low	Low
Pump Stations	Low	Med	Low	Low	Low	N/A	N/A	Med	Med	Med	Med	Low	Med	Low	Med	N/A	N/A
Headworks	Med	Med	Low	Low	Low	N/A	N/A	Low	Low	Med	Med	Low	Low	Low	Low	N/A	N/A

Once the risks have been identified, they can be either tolerated, terminated, treated or transferred. Termination or transfer of security risk is generally not an option for a lifeline utility organisation. A security risk may be tolerated if the assessed rating is very low or if the cost of mitigation is disproportionate to the risk rating. Physical security measures are intended to mitigate security risks, so this standard only considers the treatment stream of risk management.

Mitigating a risk can reduce the likelihood of a threat action or event occurring, reduce the impact or consequence if the threat action or event were to occur, or both.

2.3 Deter, detect, delay, respond

Physical security measures can mitigate risks through one or more of deterring, detecting, delaying, or responding to threat actions:

- **Deter** - The aim of deterrence is to stop or displace an intrusion before it has taken place. This is the primary goal of the whole protective security system
- **Detect** - The ability to detect an intrusion allows for the verification that something is happening to understand the nature of the event and initiate a response to it.
- **Delay** - Measures that are put in place to delay, or slow down the intrusion, increase the likelihood that the intruder is unable to reach their target before being apprehended.
- **Respond** - The response to the intrusion should ensure that the incident is stopped or, as a minimum, cannot progress any further. Also, post-incident response can provide information that reduces the risk of the incident occurring again.



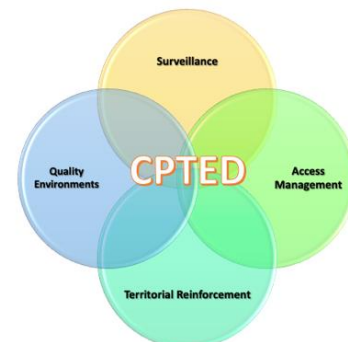
It is important to understand what domains a security measure operates within to determine how effectively it will mitigate a specific risk, if at all. For example, a CCTV camera will deter but not delay an intruder, a mechanical lock will delay but not detect an intruder, an intruder detection system (IDS) will detect and instigate a response but not delay an intruder.

2.4 Crime prevention through environmental design (CPTED)

CPTED provides a framework for incorporating crime prevention through urban design by focusing on reducing the opportunity to commit crime, therefore lessening the motivation to offend.

There are four key overlapping CPTED principles:

- **Surveillance** – people are present and can see what is going on.
- **Access management** – methods are used to attract people and vehicles to some places and restrict them from others.
- **Territorial reinforcement** – clear boundaries encourage community 'ownership' of the space.



- **Quality environments** – good quality, well maintained places attract people and support surveillance.¹

The natural and built environment can help or hinder physical security. While the origins of CPTED are in urban design, there are elements that are applicable to Watercare sites. For example, perimeter vegetation can provide privacy and block the view of attractive assets from outside the perimeter (deter), however, it can also provide natural cover for a potential intruder enabling their actions to go unseen. Thus a design should consider how the layout and landscaping helps prevent potential threats.

2.5 Security in depth

'Security-in-Depth' involves layering multiple security measures to make unauthorised access difficult. These measures should complement and support one another. A visual representation of this is shown in Figure 2.

Each individual layer represents a set of security controls or obstacles that any threat or attacker would need to breach in order to compromise the asset(s), with the layers operating cumulatively towards the total effective protection. Layers of security controls also provide redundancy, reducing the risk of compromise should a single layer fail.



Figure 2 – Layered approach to physical security.

2.6 PSR security zones

The New Zealand Government Protective Security Requirements (PSR) Framework promotes the use of security zoning as a way to identify areas of a site that require different security profiles and control measures. Security zoning is most effective when an organisation is clear about what it is trying to protect and why protecting it is important. The PSR guide to Business Impact Levels (BILs)² provides a useful conceptual framework to support this, and a Watercare-specific BIL table is provided in Appendix D. Table 3 contains descriptions of each of the PSR Security Zones relevant to Watercare.

Table 3 – PSR Security Zone descriptions

ZONE	DESCRIPTION
Zone Four	A security area with the highest level of security controls - strict control of visitors and employees on a 'Need to Access' basis, with additional security mechanisms [i.e., access card and PIN, or access card and key]. It provides access controls to information and physical assets

¹ <https://www.justice.govt.nz/assets/Documents/Publications/cpted-part-1.pdf>

² <https://www.protectivesecurity.govt.nz/governance/business-impact-levels/>

ZONE	DESCRIPTION
(Secure Area)	the loss of which would result in a business impact up to catastrophic.
Zone Three (Restricted Access Area)	A security area with high security controls, strict control of visitors on a 'Need to Access' basis, and controlled staff access. It provides access controls to information and physical assets, the loss of which would result in a business impact up to extreme. It also provides protection of people.
Zone Two (Controlled Access Area)	Areas which have unrestricted access to staff and restricted (escorted) visitor/public access. A low security area which provides access controls to information and physical assets, the loss of which would result in a business impact up to very high. It also provides some protection to people.
Zone One (Publicly Accessible/Unsecured Area)	Publicly accessible/unsecured areas including out-of-office working arrangements. It provides limited access controls to information and physical assets, the loss of which would result in a business impact of low to medium. It also provides limited protection to people.

Security zoning enables proportionate mitigation measures to be applied and provides consistency in the application of mitigation measures across areas of similar impact.

Table 4 contains a list of areas that should be classified into each Security Zone.

Table 4 – Security Zone areas

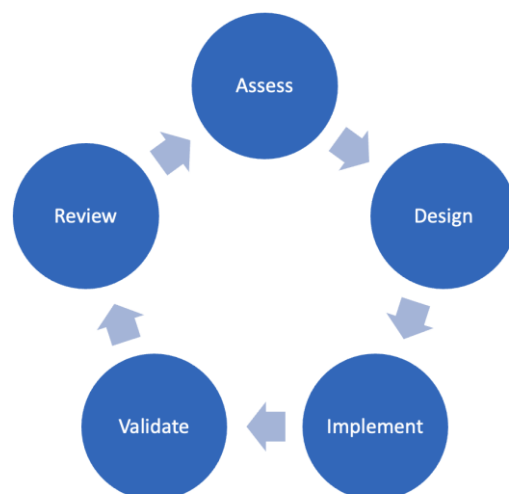
ZONE	AREA DESCRIPTION	EXAMPLES
Zone 4 (Secure Area)	<ul style="list-style-type: none"> Operationally critical areas. Areas containing sensitive information, communications or security infrastructure. Areas containing hazardous or sensitive assets. Areas housing high value assets attractive for theft. 	<ul style="list-style-type: none"> Operationally critical plant rooms. Communications/server rooms. Bulk store of hazards chemicals, direct access to high voltage. High value asset stores. Biohazard laboratories.

Zone 3 (Restricted Access Area)	<ul style="list-style-type: none"> All buildings or areas that contain equipment operationally necessary for the functioning of the site (either directly or indirectly). In practice, this is generally the bulk of the site operational areas. 	<ul style="list-style-type: none"> Control rooms. Laboratories. Water or wastewater treatment areas. Water or wastewater pumping/transportation areas. Areas containing electrical or mechanical equipment for site functions
Zone 2 (Controlled Access Area)	<ul style="list-style-type: none"> Areas that are not publicly accessible but do not contain accessible assets or information requiring heightened security measures. 	<ul style="list-style-type: none"> Office and general staff areas. The general site area within a security perimeter fence. Zone 1 areas of buildings that are secured at the end of the day. All other areas not publicly accessible or zoned higher.
Zone 1 (Publicly Accessible Area)	<ul style="list-style-type: none"> Areas accessible to the public. 	<ul style="list-style-type: none"> Reception areas (during working hours). Areas of site not contained within a security fence.

2.7 Physical security lifecycle

Like most operational areas of a business, physical security is not set-and-forget. The lifecycle of physical security can be broken down into five steps:

- Assess:** Understand the physical security requirements for the site by undertaking a threat and risk analysis, considering any site-specific risks as appropriate. Ascertain any constraints that may impact on the physical security controls that can be implemented and determine the acceptable risk tolerance level for the site.
- Design:** Determine what physical security controls are required to provide pragmatic and proportionate mitigation of the identified risks. Design the arrangement of those controls to complement each other and provide layered security-in-depth protection to the site.
- Implement:** Install the controls at the site in accordance with the risk-informed design.
- Validate:** Ensure the installed controls are operating as intended and that they are providing appropriate mitigations to the identified risks.



- **Review:** Regularly review the threat environment and the associated risks to ensure the installed controls remain effective. Where gaps are identified, undertake the lifecycle process again to enhance the physical security of the site and ensure the controls provide appropriate protection.

3. Site Specific Security Controls

Every Watercare site is different, so a one-size fits all approach to physical security controls is not appropriate. Follow the process in this section to determine what specific controls are required at a given site. The Watercare Security Team can provide assistance through any stage of this process as required.

3.1 Site-specific risk assessment

Assess the site-specific risk profile, including the appropriate levels for the baseline risks and any site-specific risks not covered by the baseline risks. Factors to consider include:

- **Site type/function** – The criticality of the site and the size of the population it serves will influence the impact aspect of operations risks. Valuable/attractive assets at the site may influence the likelihood aspect of theft related risks.
- **Site staffing** – Sites that are occupied 24/7 may be at a reduced risk of theft or vandalism but may be at an increased risk of intentional harm to staff. Sites that are normally unstaffed may be at a higher risk of theft or vandalism, but a much-reduced risk of intentional harm to staff.
- **Site location and environment** – Visibility from public areas and high traffic areas afford a level of natural surveillance and may reduce the risk of theft and vandalism. While remote sites may be at a reduced risk of opportunistic theft and vandalism, this may be offset by the potential for criminals to operate undetected.
- **Local crime statistics** – Areas with high crime rates will generally provide a heightened level for crime-related risks. The types of crime in the local area can also influence the risk levels, for instance areas with high rates of assaults may present an increased risk of intentional physical harm to site staff, particularly at night.
- **Previous security incidents on-site or at nearby/similar sites** – While history cannot predict the future, understanding previous security incidents at the site, or at nearby or similar sites, can provide valuable insight into the likely risk areas in the future.

Insight into the factors above can be gained through consultation with stakeholders, staff, Police and the local community, along with the review of security incident records.

Guidelines to assist in setting appropriate levels are contained in Appendix E.

3.2 Physical security measures required.

Physical security control measures can be applied across two categories:

- **Baseline risks:** Determine the physical security measures required to mitigate the baseline risks. Table 5 provides the starting point, with further details in Section 4 and Appendix E.

- **Site-specific risks:** Determine any additional physical security measures required to mitigate any additional site-specific risks identified. This may just involve increasing one or more security measures above the reference level standard identified from the baseline risks.

As an example, a set of baseline controls for pump stations intended to be used as a starting point for routine pump station build projects is enclosed as Appendix F. Should any deviations from this baseline be required, and for any other site type, the security team must be consulted.

Table 5 – Security controls by site type

SECURITY MEASURE	Water Treatment Plant	Wastewater Treatment Plant	Office Laboratory	Maintenance Depot	Pump Stations	Headworks
Security Culture and Training	✓	✓	✓	✓	✓	✓
Security Communication	✓	✓	✓	✓	✓	✓
Signage	✓	✓	✓	✓	✓	✓
Perimeter fence & access points	High	High	High Med	High	High Med Low	High Med Low
Site appearance and maintenance	✓	✓	✓	✓	✓	✓
Fresh water and wet well doors and hatches	✓	N/A	N/A	N/A	✓	✓
Unhoused operational assets	✓	✓	As required	✓	N/A	✓
Reception area	Med	Med	High	Med	N/A	N/A
Zone 4	✓	✓	As required	As required	N/A	N/A
Zone 3	✓	✓	✓	✓	✓	✓
Zone 2	✓	✓	✓	✓	✓	✓
Security lighting	High	High	High Med	High	High Med Low	High Med Low
CCTV	High	High	High Med	High	High Med Low	High Med Low
IDS	✓	✓	✓	✓	✓	✓
Electronic access control system (EACS)	✓	✓	✓	✓	✓	✓
SSP	✓	✓	✓	✓	✓	✓
Security Communications Network	✓	✓	✓	✓	✓	✓
Electronic Security Cabinets	✓	✓	✓	✓	✓	✓
Security Cabling	✓	✓	✓	✓	✓	✓

4. Physical Security Standards

4.1 Specific language for compliance

The standards in this document use specific language to determine the level of compliance required.

Must: Controls listed as **must** or **must not** indicate compliance is mandatory. Use of these controls may be reviewed if the control is demonstrably not relevant. Non-compliance must be supported by an assessment of the residual risk which must be accepted by the Watercare Security Manager.

Should: Controls listed as **should** or **should not** indicate compliance is considered recommended best practice. These controls should be implemented unless a valid reason exists to deviate. Non-compliance must be supported by an assessment of the residual risk which must be documented and accepted by the site manager.

Consider: Controls listed as **consider** are suggestions that may improve the overall security posture of the site. It is recommended these controls are considered in conjunction with the site risk assessment with implementation at the project manager or site manager's discretion.

OR: **OR** denotes an alternative or alternatives to the listed standard.

4.2 Beyond the perimeter (Projected security measures)

The area beyond the perimeter where protective security measures can be projected includes both the physical area around a site outside of the security perimeter and displays information such as the Watercare contact details and website.

4.2.1 Security culture and training

DESCRIPTION	Everyone in the organisation contributes to security. No amount of investment in physical security will be effective without the right security culture, which includes all users being familiar with the security controls in place.
STANDARD: ALL SITES	All staff, contractors and consultants must undertake training on the purpose and operation of security control measures (e.g. IDS) employed at sites where they have unescorted access.
	All staff, contractors and consultants must undertake general security awareness training.

4.2.2 Security communication

DESCRIPTION	Information which can be obtained without breaching the site or building perimeter can indicate the presence of valuable assets or provide information useful in bypassing or defeating security control measures. Conversely, it can also imply that security is taken seriously and the control measures in place are effective.
-------------	--

STANDARD: ALL SITES	The Watercare website, must not contain information that can be used to degrade, bypass or defeat site security control measures.
	The Watercare website should contain information that implies the security of the site is taken seriously and there are effective security control measures in place.
	Signage visible from the perimeter or beyond the perimeter, such as site maps or hazard boards, should not indicate the presence or location of critical, sensitive, high value or attractive items or areas.

4.2.3 Signage

DESCRIPTION	Security signs inform the area beyond the perimeter fence (or gate or door, as appropriate) is not a public space and only authorised persons should enter. They also inform of the potential consequences should an unauthorised person enter. Security signs potentially deter unwanted activity by increasing the perceived risk of consequences from criminal activity. Signs also inform of the presence of CCTV cameras where these are installed. Appropriate CCTV signage is an important component of complying with the Privacy Act 2020.
STANDARD: ALL SITES	Restricted access signs, including CCTV warning signs as appropriate, must be displayed at all access points and at other appropriate points around the site perimeter.
	Signs must state the area beyond the fence/gate/door is a restricted place and indicate the consequences of unauthorised access (Figure 3 and Figure 4). ³
	There should also be signs clearly marking where visitors should enter the site and how they gain access (e.g. with an intercom at the gate), along with the path to where they need to sign in.



Figure 3 - Example CCTV warning sign.



Figure 4 - Example Restricted Access sign.

³ Standard design security signage is available from the Watercare Security Team.

4.3 Perimeter

The perimeter is the demarcation between public and private space. In most cases, where public access to the site is not desirable, the perimeter also forms the first layer of security to protect the assets contained within the site.

4.3.1 Perimeter fencing

DESCRIPTION	Security fencing is designed to deter, delay and detect unauthorised access to a site. At a minimum, perimeter fencing marks the site boundary to deter or discourage unnecessary access, utilising the CPTED principal of territorial reinforcement. In most cases, perimeter fencing is intended to provide a sufficient physical barrier to delay or deny unauthorised site access.
HIGH SECURITY FENCE	A high security fence should deter all but the most determined intruder from attempting to gain access to the site and provides an alert to monitoring staff if an attempt to gain entry through or over the fence. High security perimeter fencing should be used to protect water and wastewater treatment plants, pump stations in remote or high crime areas and other sites that contain high value or hazardous assets.
STANDARD:	<p>The perimeter fence must be chain link with steel poles, including top and bottom rails OR concrete OR concrete block OR steel palisade (Figure 5, Figure 6 and Figure 7).</p> <p>It must be a minimum of 1.8 m high and topped with three strands of barbed wire and flat coils of razor wire OR a minimum of 2.2 m high topped with steel spikes.</p> <p>It must incorporate fence sensors OR be backed with zoned monitored pulse electric fence⁴.</p> <p>Building exterior walls can form some, or all, of a site perimeter, but care must be taken to avoid potential climbing aids.</p> <p>Anti-climb measures (barbed/razor wire) should be used on single storied buildings where climbing could provide site access.</p> <p>A zone of 3 m (ideal) or 1.5 m (where appropriate) on either side of perimeter fence must be kept clear of vegetation or structures that could be used as climbing aids or surveillance blind spots.</p>
MEDIUM SECURITY FENCE	A medium security fence should mark the site boundary and require a medium level of effort to circumvent. It will deter an undetermined intruder but will provide minimum delay to a motivated intruder. Medium security fence can be used on the wider perimeter of water or wastewater treatment plants where an inner high security fence is in place around operational areas. It can also be used at pump stations or other sites where there is a low risk of vandalism, and all operational plant or valuable/hazardous assets are within a secure building structure.

⁴ **Consider** de-energising or applying low voltage to the electric fence when the site is occupied.

STANDARD:	The perimeter fence must be chain link OR wooden/steel palisade OR wire panel trellis OR equivalent (Figure 8).
	It must be a minimum of 1.5 m high.
	Anti-climb measures are not required.
LOW SECURITY FENCE	A low security fence provides boundary marking with little deterrent effect. It should be used only on pump stations in low crime areas where the risk of vandalism is very low and all assets are contained within a secure building structure, and where general public pedestrian access to the site is acceptable.
STANDARD:	The perimeter fence should be a low wooden post fence OR wire stock fence OR equivalent.
NO SECURITY FENCE	No security fence should only be used where land ownership or similar considerations dictate a fence cannot be installed. This should only be applied to pump stations in low crime areas where the risk of vandalism is very low and all assets are contained within a secure building structure, and where general public pedestrian access to the site is acceptable.
STANDARD:	No Fence
FENCES SURROUNDING OPEN BODIES OF WATER	Open bodies of water, such as wastewater settlement ponds, pose a risk of accidental drowning. Appropriate perimeter fencing should be used to mitigate this risk by restricting access to these bodies of water. It should be noted that this standard is specifically a health and safety requirement but included in the perimeter fencing section of this security standards document for completeness. This standard represents the minimum requirement for containing open bodies of water. Where both a security and health and safety requirement exist, the greater of the two standards should be applied.
STANDARD:	The perimeter fence must be X Fence Netting security fence OR an equivalent self-supporting or supported mesh fencing OR an equivalent fence or barrier that prevents easy access to the open body of water.
	It must be a minimum of 1.8 m high and topped with three strands of barbed wire OR equivalent anti-climb measures.
	It must not contain gaps greater than 100 mm between the fence and the ground or other supporting structures. It must be installed in such a way as to prevent lifting or other means of passing beneath the fence structure.
	Building exterior walls can form some, or all, of the perimeter, but care must be taken to avoid potential climbing aids.
	A zone of 3 m (ideal) or 1.5 m (where appropriate) on either side of perimeter fence must be kept clear of vegetation or structures that could be used as climbing aids.



Figure 5 – Example high security fence.



Figure 6 – Example alternative high security fence.

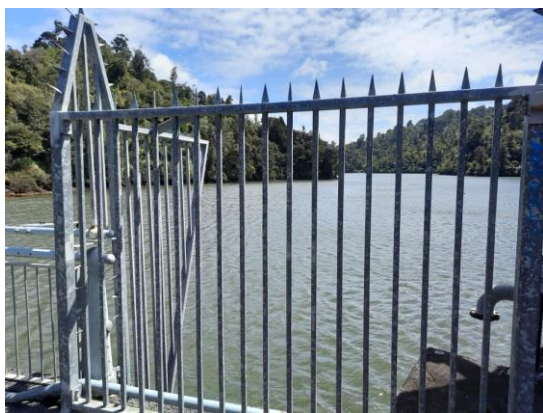


Figure 7 – Example alternative high security fence.



Figure 8 – Example medium security fence.

4.3.2 Perimeter access points

DESCRIPTION	Perimeter access points provide authorised vehicle and pedestrian access to the site. It is important that access do not introduce weakness or vulnerabilities in the wider site perimeter security.
STANDARD: ALL SITES	<p>Perimeter access points must provide at least the same level of security protection as the remaining perimeter security measures that contain them.</p> <p>The number of access points in a site perimeter should be kept to a minimum with consideration to operational and potential evacuation requirements.</p> <p>Vehicle and pedestrian access gates must be constructed to the same or higher standard as the fence that contains them.</p> <p>Also refer to the Security Lighting, CCTV and EACS standards.</p>
STANDARD: HIGH	High security vehicle access points must be used where a high security fence is in place.

SECURITY VEHICLE ACCESS POINTS	Primary vehicle access points for sites that are normally occupied or regularly visited must be a motorised sliding gate (Figure 9).
	The gate must be integrated into the EACS and secured with a magnetic lock, with swipe in and out.
	Entry after-hours should require dual authentication.
	Motorised swing gates should only be used where installing a sliding gate is not possible.
	Gate opening times should be set to the minimum required for a vehicle to safety pass through to reduce the risk of tailgating.
	Space should be available on either side of the gate to allow a vehicle to stop and wait for the gate to close before moving on.
	Primary access points for sites that are not normally occupied or regularly visited, and other access points that are not regularly used, should be a manual swing or sliding gate secured with a padlock.
STANDARD: HIGH SECURITY PEDESTRIAN ACCESS POINTS	High security pedestrian access points must be used where a high security fence is in place.
	Access points that are regularly used by pedestrians must be a manual single leaf swing gate with an automatic closer (preferred) or a motorised single leaf swing gate (Figure 10).
	The gate must be integrated into the EACS and secured with a magnetic lock, with swipe in and out.
	Entry after-hours should require dual authentication.
	Motorised gate opening times should be set to the minimum required for a person to safety pass through to reduce the risk of tailgating.
	Signs warning of tailgating should be displayed on both entry and exit.
	Access points that are not regularly used should be a manual swing gate secured with a padlock.
STANDARD: MEDIUM SECURITY VEHICLE ACCESS POINTS	Medium security vehicle access points must be used where a medium security fence is in place.
	Vehicle access points must be manual swing or sliding gates secured with a padlock (Figure 11).
STANDARD: MEDIUM SECURITY PEDESTRIAN ACCESS POINTS	Medium security pedestrian access points must be used where a medium security fence is in place.
	Pedestrian access points must be manual swing gates secured with a padlock (Figure 10).

STANDARD: LOW SECURITY VEHICLE ACCESS POINTS	Low security vehicle access points should be used where a low security fence is in place.
	Even when no fence is in place, a low security vehicle access point should be installed to prevent unauthorised vehicle access to the site.
	The vehicle access point should have a stock gate OR steel pole barrier arm OR equivalent secured with a padlock (Figure 12).
STANDARD: LOW SECURITY PEDESTRIAN ACCESS POINTS	Low security pedestrian access points should be used where a low security fence is in place.
	The pedestrian access point should be a gap in the fence of sufficient size to allow a pedestrian (or bicycle, pushchair or wheelchair as appropriate) to pass through.

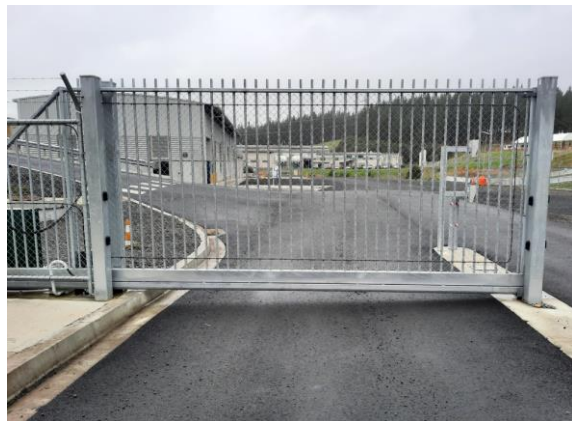


Figure 9 – Example high security vehicle access point.



Figure 10 – Example high security (left) and medium security (right) pedestrian access points.



Figure 11 – Example medium security vehicle access point.



Figure 12 – Example low security vehicle access point.

4.4 Site (including reservoirs)

The site includes all areas within the perimeter or boundary, including car parks, roads, and open storage areas, along with the grounds and vegetation.

4.4.1 Site appearance and maintenance

DESCRIPTION	A site that appears tidy and well maintained provides a projection of control and order as well as encouraging a sense of community pride and ownership, which acts as a deterrent to criminal activity.
STANDARD: ALL SITES	All sites should be configured to reduce the opportunities for vandalism (for instance graffiti) by avoiding solid fencing where possible (concrete, wooden pale) and using building styles that deter graffiti.
	The site should be regularly maintained to give an impression of control, order and a sense of care and ownership.

4.4.2 Fresh water and wet well doors and hatches

DESCRIPTION	Doors and inspection hatches, or other means that allow direct access to drinking water, potentially provide the ability to contaminate the water supply. In the worst case, the introduction of contamination to the drinking water supply may result in adverse health effects on customers. Even if there is no associated health risk, contamination risks reputational damage to Watercare and a loss of confidence in the water supplied. Likewise, access to raw sewage introduces biohazard risks.
STANDARD: ALL SITES	All access points that provide access to drinking water (e.g. reservoir inspection hatches) or raw sewage (e.g. doors to wet wells) must be fitted with sensors (e.g. reed switch) that provide an alert to the Nerve Centre when they are opened (Figure 13).
	All access points must be physically secured. The minimum is a non-standard fitting (such as a Crox bolt).
	Access points that are publicly accessible must be secured with a mechanical lock, with preference given to keyed locks in doors or a steel bar laid over the centre of the hatch cover secured in place with a padlock.

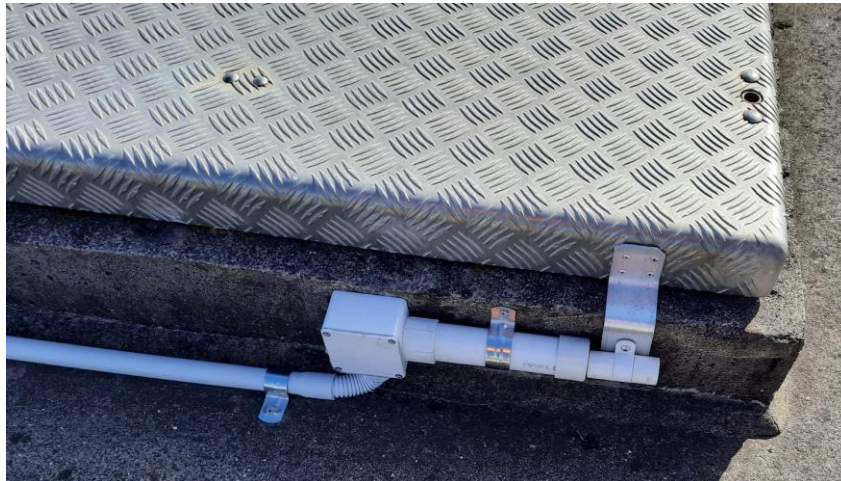


Figure 13 – Fresh water hatch secured with Clix bolts and fitted with a self-test reed switch.

4.4.3 Unhoused operational assets

DESCRIPTION	Unhoused assets within the site that are operationally important or critical and would otherwise be stored in or classified as Zone 3 or 4 (see PSR Security Zones below) but are not contained within a building or other structure. This may include unhoused water sources, valves, generators, or control equipment.
STANDARD: ALL SITES	Unhoused operational assets must have additional security control measures in place in accordance with their operational criticality.
	Important or critical assets should be contained within an appropriate building or structure whenever possible.
	An additional layer of high security perimeter fence should be employed to prevent access to unhoused operational assets.

4.5 Buildings

Buildings can be loosely categorised into two types – operational and storage/other. Operational buildings include those that contain operational plant, office and other staff working areas, and areas that contain maintenance or other functions critical to the operation of the site. Storage/other areas include sheds, storage and other areas not critical to the operation of the site.

4.5.1 Reception areas

DESCRIPTION	Reception areas are where there is regular interaction with members of the public. They present a heightened risk of harm to staff from aggressive or violent issues, or motivated acutely disaffected persons. As such, additional security controls are required to ensure the safety of staff, contractors and other members of the public.
STANDARD: ALL SITES	<p>The staff side of the reception desk must not be freely accessible from the public space.</p> <p>Any doors between the public and staff sides of the desk must be access controlled.</p> <p>All areas of reception and the public approach must be visible by reception staff, using CCTV and monitors if required.</p>
HIGH RISK SITES	High risk sites are those that regularly deal with members of the public or where members of the public have uncontrolled access to the reception area
STANDARD:	<p>Reception desks must be designed to make it difficult to climb over while maintaining a welcoming posture. Measures to achieve this should include the height of the desk, width of the counter and physical barriers on and/or above the counter.</p> <p>Loose items must not be available on the desk that could be used as a projectile or weapon.</p> <p>Items such as monitors must be fixed to the desk or another structure.</p> <p>Keyboards, mice and other peripherals should be out of reach from the public side.</p> <p>Staff must have a safe retreat route to a secure area that can be utilised in the event of an incident in the reception area.</p> <p>A duress alarm system should be implemented which alerts other site staff and the Nerve Centre when triggered, with a fixed (preferred) or mobile activation switch under the reception desk (preferred) or otherwise easily accessible by reception staff.</p> <p>A CCTV camera or cameras must be in place that is able to identify individuals on the public side of the reception desk.</p>

MEDIUM AND LOW RISK SITES	Medium and low risk sites are those that do not regularly deal with members of the public or where members of the public do not have uncontrolled access to the reception area, such as when site staff must provide access through a gate or door before the reception area can be accessed.
STANDARD:	<p>Reception desks should be designed to make it difficult to climb over while maintaining a welcoming posture. Measures to achieve this should include the height of the desk, width of the counter and physical barriers on and/or above the counter (Figure 14).</p> <p>Loose items should not be available on the desk that could be used as a projectile or weapon.</p> <p>Items such as monitors should be fixed to the desk or other structure.</p> <p>Keyboards, mice and other peripherals should be out of reach from the public side.</p> <p>Staff should have a safe retreat route to a secure area that can be utilised in the event of an incident in the reception area.</p> <p>Consider implementing a duress alarm system which alerts other site staff and the Nerve Centre when triggered, with a fixed (preferred) or mobile activation switch under the reception desk (preferred) or otherwise easily accessible by reception staff.</p> <p>Consider installing a CCTV camera or cameras in place that is able to identify individuals on the public side of the reception desk.</p>



Figure 14 – Example medium risk site reception desk.

4.5.2 PSR security zones

	ZONE 4	ZONE 3	ZONE 2
DESCRIPTION	A security area with the highest level of security controls - strict control of visitors and employees on a 'need-to-access' basis, with additional security mechanisms (e.g. access card and PIN, or access card and key). It provides access controls to information and physical assets the loss of which would result in a business impact up to catastrophic.	Areas which are restricted to staff with a valid need-to-access. Visitors must be escorted or closely controlled. A high security area which provides access controls to information and physical assets, the loss of which would result in a business impact up to extreme. It also provides protection to people.	Areas which have unrestricted access to staff and restricted (escorted) visitor/public access. A low security area which provides access controls to information and physical assets, the loss of which would result in a business impact up to very high. It also provides some protection to people.
AREAS	<ul style="list-style-type: none"> • Communications/ server rooms. • Operationally critical and/or hazardous/sensitive areas (e.g. bulk store of hazards chemicals, direct access to high voltage). • Areas housing high value assets attractive for theft (e.g. high value asset stores). 	<p>All buildings or areas that contain equipment operationally necessary for the functioning of the site (either directly or indirectly) should be classified as Zone 3 areas e.g.:</p> <ul style="list-style-type: none"> • Control rooms, laboratories, • Water or wastewater treatment areas, • Water or wastewater pumping/ • Transportation areas • Areas containing electrical or mechanical equipment for site functions. <p>Generally all areas other than Zone 4 areas, staff office and amenity areas or public areas.</p>	All other areas not publicly accessible or zoned higher normally encompassing office and general staff areas. In general, the area within a secure site perimeter fence will be considered Zone 2 and publicly accessible (Zone 1) areas of buildings revert to Zone 2 when the building is secured at the end of the day.
BOUNDARY CONSTRUCTION	Zone 4 areas must be constructed to resist intrusion.	Zone 3 areas should be constructed to resist intrusion.	

ZONE 4		ZONE 3	ZONE 2
	Internal walls and ceilings must be “slab-to-slab”		
	Walls should be lined with 18 mm plywood in addition to plasterboard, or with equivalent intrusion resistant materials.	Walls should be constructed to a high quality commercial standard and maintained to that level.	Walls should be constructed to a normal commercial standard and maintained to that level.
	Windows (both internal and external) should be avoided where possible.	External windows should be avoided where possible.	
	External windows must have steel security bars or grills installed (Figure 15).	External windows should have steel security bars or grills installed.	
	External windows must have privacy film installed.	External windows should have privacy film installed.	External windows where the public could oversee work environment should have privacy film installed.
	Any opening window must be permanently fixed closed.	Any opening window should be permanently fixed closed or fitted with a window stay and keyed window lock.	Externally opening windows must have window stays and should have keyed window locks.
	Windows at high risk of vandalism, such as those immediately accessible to public spaces, should be laminated glass or have anti-shatter film applied.		
	Internal windows should have steel security bars or grills installed along with privacy film.		

DOORS	Access point doors must be resistant to intrusion and be fitted with heavy duty two or three stage automatic door closers (Figure 16).		Access point doors should be normal commercial standard fitted with heavy duty two or three stage automatic door closers.
	Access doors from internal lower security zones areas must be minimum 38 mm solid core wooden doors (or equivalent) hung on three or four evenly spaced fixed/captured pin hinges in steel (preferred) or solid wood frames.		
	External doors must be steel lined minimum 38 mm solid core wooden doors (or equivalent) hung on three or four evenly spaced fixed/captured pin hinges in a steel (preferred) or solid wood frame,	External doors must be minimum 38 mm solid core wooden doors (or equivalent) hung on three or four evenly spaced fixed/captured pin hinges in steel (preferred) or solid wood frames (Figure 17).	
	Doors must be outwards opening unless they are required to be inwards opening for fire escape/evacuation purposes.		Doors should be outwards opening unless they are required to be inwards opening for fire escape/evacuation purposes.
	External outward opening doors must be fitted with three evenly spaced hinge bolts.	External outward opening doors should be fitted with three evenly spaced hinge bolts.	
	Fire escape/evacuation paths must avoid passing through Zone 4 areas whenever possible.	Fire escape/evacuation paths should avoid passing through Zone 3 areas whenever possible.	

LOCKS AND ACCESS CONTROL	Zone 4 perimeter access points must be integrated into the site EACS using electronic mortice or magnetic locks (Figure 18).	Perimeter access points should be integrated into the site EACS using electronic mortice or magnetic locks.	
	Dual authentication (swipe and PIN) must be required for entry with swipe to exit.	Dual authentication (swipe and PIN) should be required for entry with swipe to exit (Figure 19).	Dual authentication (swipe and PIN) should be required for entry outside normal operating hours.
	Access must only be provided to staff and contractors on a strict need-to-access basis.		Access should only be provided to staff and contractors on a need-to-access basis.
	Door-open-too-long alarms must be enabled with local audible alarms, along with alerts at the Nerve Centre after-hours.	Door-open-too-long alarms should be enabled with local audible alarms, along with alerts at the Nerve Centre after-hours.	Consider enabling door-open-too-long alarms with local audible alarms, along with alerts at the Nerve Centre after-hours.
	Forced door and emergency door release must be enabled with local audible alarms and trigger alerts at the Nerve Centre at all times.	Forced door and emergency door release should be enabled with local audible alarms and trigger alerts at the Nerve Centre at all times.	
	Zone 4 areas must be secured with mechanical deadbolt locks after-hours using a restricted profile key within the Watercare key management system.	External Zone 3 access points must be secured with mechanical deadbolt or padlocks after-hours using a restricted profile key within the Watercare key management system.	External Zone 2 access points should be secured with mechanical deadbolt or padlocks after-hours using a restricted profile key within the Watercare key management system.
	The primary leaf of two-leaf doors must meet the requirements above with the secondary leaf being mechanically locked any time it is not in use using flush and/or door bolts. Secondary leaf mechanical locks must not be accessible without access first being granted through the primary leaf.		
IDS	Zone 4 areas must be protected by an Intruder Detection System (IDS).	Zone 2 and 3 areas should be protected by an Intruder Detection System (IDS) (Figure 20).	
	Full area volumetric movement sensors should be installed.	Consider installing full area volumetric movement sensors.	

	Zone 4 areas must be armed anytime they are not occupied.	Zone 3 areas must be armed outside normal hours of operation.	Zone 2 areas should be armed outside normal hours of operation.
	The IDS panel for the zone must be within a Zone 4 area and covered by IDS sensors.	The IDS panel for the zone must be within a Zone 3 or 4 area and covered by IDS sensors.	The IDS panel for the zone must be within a Zone 2, 3 or 4 area and covered by IDS sensors.
	Zone 4 areas should be on a dedicated IDS zone.	A timed auto-arm should be used as a backup in the event staff forget to manually arm the area but must not be used as the default arming process.	Consider using a timed auto-arm process.
CCTV	Access points to Zone 4 areas should have CCTV coverage.	Consider CCTV coverage of access points to Zone 3 areas.	Consider CCTV coverage of external access points to Zone 2 areas.



Figure 15 – Window with steel security bars.



Figure 16 – Heavy duty door closer.



Figure 17 – Example solid core wood door.



Figure 18 – Magnetic clamp lock.



Figure 19 – External card reader with keypad.

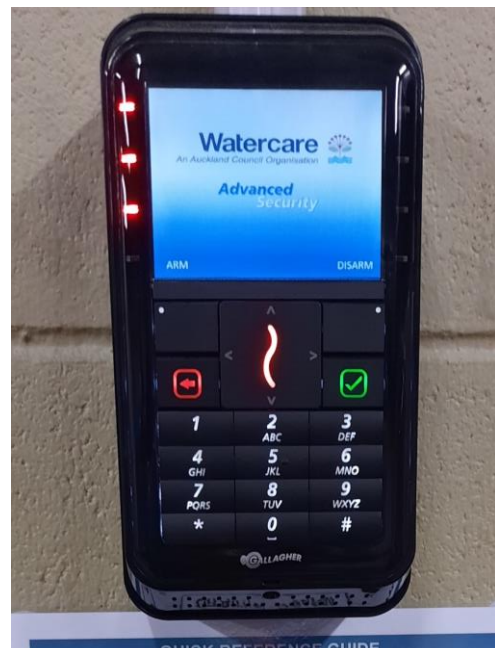


Figure 20 – IDS keypad.





4.6 General

4.6.1 Security lighting



DESCRIPTION	Security lighting provides an additional layer of protection for people and assets during times of darkness and should provide sufficient illumination over an area to ensure anyone moving in or around it can be seen. Effective security lighting can deter as well as detect unwanted activity, along with reducing the risk of harm by enabling visibility and situational awareness, particularly around access points. Note that the standard below is the minimum required for security purposes. Additional lighting may be required for Health and Safety purposes.
STANDARD: ALL SITES	Security lighting must compliment areas monitored by CCTV cameras where applicable.
	Where possible, security lighting should be located within the site perimeter and at a sufficient height to reduce the risk of vandalism.
	Motion activated LED lights should be used where possible to reduce energy consumption and light pollution to neighbouring properties. Where motion activation is not practical or appropriate, timed switches should be used, or manually switched if this is the only practical option
STANDARD: HIGH RISK SITES	Security lighting must fully illuminate all perimeter access points and approaches, and all areas of the perimeter easily accessible to the public.
	Security lighting should illuminate all areas of perimeter.
	Areas containing critical plant, high value items or items attractive for theft that are accessible (not within a building) must be illuminated by security lighting.
	General security lighting should illuminate the full site.
	Operational building access points must be illuminated by security lighting.
	The full perimeter of operational buildings should be illuminated.
	Access points of other buildings that might be used during the hours of darkness must be illuminated.
STANDARD: MEDIUM RISK SITES	Security lighting must fully illuminate the primary perimeter access points and approaches which may be used after hours.
	Security lights should illuminate areas of the perimeter easily accessible to the public.
	Security lighting should provide general illumination to the full site.
	Operational building access points that might be used during the hours of darkness must be illuminated by security lighting.
	Consider illuminating the full perimeter of operational buildings.

STANDARD: LOW RISK SITES	Security lighting should fully illuminate primary perimeter access points and approaches which may be used after hours, however, may not be required if general site and surrounding lighting provides sufficient illumination.
	Consider security lighting that provides general illumination the full site.
	Any building access point that may be used during the hours of darkness should be illuminated.

4.6.2 CCTV

DESCRIPTION	CCTV cameras and signage deters criminal activity by increasing the perceived risk of being seen. Recorded CCTV footage aids in post-incidence response (e.g. investigation). CCTV only provides detect and immediate response capability if it is viewed in real time, either by an operator monitoring a camera feed, or being prompted to view footage through smart analytical software or other alerts (e.g. fence sensor or IDS alarm).		
	CCTV cameras can be categorised into the capability groups shown below.		
			
Monitor To enable viewing of the number, direction and speed of movement of people across a wide area, providing their presence is known to the operator. <i>12.5 pixels/m</i>	Detect To enable the operator to reliably and easily determine whether or not any target (e.g. a person or vehicle) is present. <i>25 pixels/m</i>		
			
Observe To enable characteristic details of an individual, such as distinctive clothing to be seen, whilst allowing a view of activity surrounding an incident. <i>62.5 pixels/m</i>	Recognise To enable the operator to determine with a high degree of certainty whether or not an individual shown is the same as someone they have seen before, or establish the colour, make and model of a vehicle. <i>125 pixels/m</i>		



 <p>Identify To enable identification of an individual beyond reasonable doubt or read a vehicle number plate. <i>250 pixels/m</i></p>	 <p>Inspect To enable distinctive features of an individual, such as eye colour, jewellery and tattoos, to be seen. <i>1000 pixels/m</i></p>
<p>STANDARD: ALL SITES</p>	<p>CCTV systems must always be installed and used in accordance with the Watercare CCTV policy and the Privacy Act 2020.</p> <p>Appropriate CCTV signage must be displayed at any site where CCTV is in operation.</p> <p>Areas identified as containing valuable items or items attractive for theft by authorised users (staff and contractors) should have appropriate CCTV coverage.</p> <p>Access points to Zone 4 areas should be covered (minimum <i>Recognise</i>, ideally <i>Identify</i>).</p>

STANDARD: HIGH RISK SITES	High risk sites must have CCTV camera coverage of perimeter access points that are regularly used (minimum <i>Recognise</i> , ideally <i>Identify</i>).
	All access points should be covered (minimum <i>Observe</i> , ideally <i>Recognise</i>).
	Perimeter areas presenting a high risk of unauthorised access should be covered, such as areas that are easily accessible but not easily seen from general public spaces (minimum <i>Detect</i> , ideally <i>Observe</i>).
	Where fence sensors are installed, Pan/Tilt/Zoom cameras should be used to provide coverage of perimeter fence zones that can be used in response to an alarm (minimum <i>Recognise</i> , ideally <i>Identify</i>).
	Areas containing critical plant, high value items or items attractive for theft that are accessible (not within a building) must be covered by CCTV cameras (minimum <i>Recognise</i> , ideally <i>Identify</i>).
	Operational building access points must be covered (minimum <i>Recognise</i> , ideally <i>Identify</i>).
	Operational building points vulnerable to unauthorised access (e.g. accessible windows) should be covered (minimum <i>Observe</i> , ideally <i>Recognise</i>).
	Consider coverage of the full perimeter of operational buildings (minimum <i>Detect</i> , ideally <i>Observe</i>).
	Other building access points should be covered (minimum <i>Observe</i> , ideally <i>Recognise</i>).
STANDARD: MEDIUM RISK SITES	Medium risk sites should have CCTV coverage of access points that are regularly used (minimum <i>Recognise</i> , ideally <i>Identify</i>).
	Medium risk sites should have CCTV coverage of perimeter areas presenting a high risk of unauthorised access, such as areas that are easily accessible but not easily seen from general public spaces (minimum <i>Detect</i> , ideally <i>Observe</i>).
	Consider coverage of the wider site to provide general situational awareness (minimum <i>Detect</i> , ideally <i>Observe</i>).
	Operational building access points and points vulnerable to unauthorised access (e.g. accessible windows) should be covered (minimum <i>Observe</i> , ideally <i>Recognise</i>).
STANDARD: LOW RISK SITES	Low risk sites are unlikely to require CCTV.

4.6.3 IDS

DESCRIPTION	An Intruder Detection System (IDS) detects unauthorised access to a building or other area. When triggered, a local alarm sounds along with an alert being raised at the monitoring centre. This provides an element of deterrence and enables an appropriate response to be actioned.
STANDARD: ALL SITES	The IDS must monitor all perimeter access points to the protected area through both volumetric movement sensors e.g. passive infrared sensor (PIR) and break surface door sensors (reed switch).
	All IDS panels, keypads and sensors (PIRs, reed switches) must have tamper switches installed.
	Tamper switches must be configured to the system zone and require an administrator access to disable or bypass.
	Tamper switches must provide an alert at the monitoring centre when triggered, even when the IDS zone is unarmed.
	The IDS control panel should be located in the most secure area of the site.
	The keypad to arm and disarm an IDS zone must be covered by the zone IDS sensors.
	The IDS must require two-factor authentication (swipe and PIN) to disarm.
	The IDS should require two-factor authentication (swipe and PIN) to arm.
	The IDS must be monitored 24/7.
	The IDS should be monitored by the Nerve Centre.
	Also refer to the PSR Security Zone standards.

4.6.4 EACS

DESCRIPTION	An Electronic Access Control System (EACS) enables access to integrated doors and gates to be electronically controlled and centrally administered. Access for any user can be granted or removed electronically without the requirement to change keys or combinations. It delays and detects unauthorised access attempts. Those with access, along with all access attempts (successful and unsuccessful) can be centrally audited.
STANDARD: ALL SITES	All EACS card readers, keypads and locking devices (magnetic and mortice locks) must have tamper monitoring installed.
	Tamper detection should be monitored by the Nerve Centre.
	All doors secured with EACS must be configured to allow unhindered egress in the event of a power or system failure, or in an emergency evacuation. Examples include electronic mortice locks configured to 'fail safe' on the internal side or magnetic clamp locks fitted with an emergency exit button. (if there's a failure in the system, personnel can still exit the area – access to egress but not entry to facilities)

	All doors secured with EACS should be configured to prevent unauthorised access in the event of a power or system failure. Examples include electronic mortice locks configured to 'fail secure' on the external side or magnetic clamp locks connected to battery backup systems. (if there's a failure in the system, persons cannot enter the site)
	EACS gate locks must have a manual override on the internal/secure side of the gate to enable emergency exit in the event of power loss.
	EACS gate lock manual overrides must not be accessible from the external/insecure side of the gate.
	Also refer to the PSR Security Zone standards.

4.6.5 SSP

DESCRIPTION	A Site Security Plan (SSP) documents site-specific security information, for example information on the IDS and CCTV systems, key management and auditing processes, visitor and contractor management protocols, emergency procedures and review processes.
STANDARD: ALL SITES	All sites must have a SSP – this document shall be developed in consultation with the security team after which it is owned, reviewed and updated by the facility.
	SSPs should be informed by, and complimentary to, the wider suite of Watercare security documentation.
	A site-specific threat assessment and security risk register should be included in the SSP.
	The SSP must include processes to respond to a heightened threat environment, including changes to physical security measures that may need to be implemented in the event of a pending or in-progress security incident. An example of a basic Alert Level system is included in Appendix F.
	The SSP should include lockdown processes and procedures, including clear guidance on when a lockdown should be activated and who has the authority to authorise it.
	The response to heightened threat environments and lockdowns should be regularly reviewed and exercised to ensure they remain fit for purpose and staff are aware of the processes.
	SSPs must be reviewed at least bi-annually, or when significant changes to the operating environment or security requirements are applicable to ensure they remain fit for purpose.

4.6.6 Security communications network

DESCRIPTION	Remote monitoring of the electronic security systems, such as IDS, EACS and CCTV, require a network over which critical information can be communicated.
-------------	--

	The preferred method to achieve this is using the Watercare corporate network infrastructure as a transport medium.
STANDARD: ALL SITES	All sites must have security communications network connectivity.
	Sites should have a connection to the Watercare corporate network infrastructure as the preferred transport medium for security communications.
	Remote viewing of CCTV footage requires significantly more network bandwidth than basic security system monitoring alone. Sites with CCTV must consider bandwidth when provisioning network connectivity.
	Watercare Digital must be consulted when planning and implementing security communications into the corporate network to ensure current network standards are met.

4.6.7 Electronic security cabinets

DESCRIPTION	Electronic security systems, such as IDS, EACS and CCTV, require control infrastructure. This is normally contained within a wall-mounted cabinet inside a building on site. Larger sites with multiple buildings may require several security cabinets. Security cabinets generally require a dedicated single 240V/10A mains power outlet.
STANDARD: ALL SITES	All sites must have provision for a wall-mounted security cabinet with an associated mains power outlet.
	The security cabinet must be in an area protected by an IDS.
	The security cabinet should be located in the most secure area of the site, for instance a server or communications room.
	The security cabinet power should be connected to the site Uninterrupted Power Supply (UPS) and/or backup power, if available.
	The Watercare preferred security integrator must be consulted on security cabinet and power requirements during the design phase of significant site development or new builds.

4.6.8 Security cabling

DESCRIPTION	Cabling for electronic security systems, such as IDS, EACS and CCTV, needs to be installed in such a way as to reduce the risk of tampering, degradation and failure, or electrical interference.
STANDARD: ALL SITES	All security cables must be supported (e.g. catenary wire, cable trays or conduit).
	Security cables must be separated from mains power cable by at least 300 mm.
	The corrosive nature of the environment in operational areas must be recognised with the installation of security cables (e.g. through the use of stainless steel fittings).

Appendix A – Useful References

A list of relevant and useful legislation, policies and standards are listed below.

NATIONAL LEGISLATION AND POLICY

- Health and Safety at Work Act (2015)
- Privacy Act (2020)
- Building Act (2004)
- The New Zealand Building Code
- Protective Security Requirements (PSR) framework
- New Zealand Information Security Manual (NZISM)

STANDARDS, HANDBOOKS AND GUIDES

- ISO 31000:2018 Risk management – Guidelines
- HB167:2006 Security Risk Management Handbook
- AS 1725.1-2010 Chain link fabric fencing, Part 1: Security fences and gates — General requirements
- AS/NZS 2201.1:2007 Intruder alarm systems – Client's premises – Design, installation, commissioning and maintenance
- AS 4145.2:2008 Locksets and hardware for doors and windows – Mechanical locksets for doors and windows in buildings
- AS/NZS IEC 60839-11-1:2019 Electronic access control systems
- IES G-1-16 Guide for Security Lighting for People, Property and Critical Infrastructure

Appendix B – Current Threat Assessment

The current assessed threats faced by Watercare are shown in Table 6, with the threat level definitions shown in Table 7. These threats and levels are based on a threat assessment completed in 2020.⁵ Note that these are high-level, organisational-wide threats and site-specific threat levels may vary.

Table 6 – Watercare threat levels

THREATS		THREAT LEVEL
Terrorism	International extremists	MEDIUM
	Domestic extremists	MEDIUM
Disruptive activity	Protestors, activists or issue motivated groups	MEDIUM
	Fixated or acutely disaffected persons	MEDIUM
Sabotage / unauthorised disclosure of information	Insiders	MEDIUM
	Hostile intelligence activity	VERY LOW
	Media / investigative journalism	LOW
General crime	Violence, theft and vandalism	HIGH
	Organised criminal activity	LOW
Economic crime	Cybercrime	HIGH

Table 7 – Threat level definitions.

THREAT LEVEL	DEFINITION
Extreme	A security incident impacting Watercare, its assets, information or personnel, is expected.
High	A security incident impacting Watercare, its assets, information or personnel, is assessed as highly likely.
Medium	A security incident impacting Watercare, its assets, information or personnel, is assessed as feasible and could well occur.
Low	A security incident impacting Watercare, its assets, information or personnel, is assessed as a realistic possibility.
Very Low	A security incident impacting Watercare, its assets, information or personnel, is assessed as unlikely.

⁵ Watercare_001_PSTA_2020.

Appendix C – Baseline Risks

Descriptions of terms used in the table of baseline risks (Table 2) are listed below.

RISK TYPE

Theft	The unlawful removal of property assets.
Vandalism	Damage to property assets, including buildings, plant, machinery and tools.
Contamination of water	The introduction of contaminants to the fresh drinking water supply after treatment, resulting in contaminated water being delivered to customers. Contamination levels may range from undetectable with no adverse health effects (but may cause reputational damage) through to contaminated water causing customers to get severely ill.
Release of wastewater	The unintended or unplanned release of untreated or partially treated wastewater into the local environment, which could include suburban areas or waterways.
Intentional harm	Violent or aggression behaviour towards a person causing bodily harm.

BUSINESS IMPACT

Financial loss	Watercare incurring unexpected additional costs, most likely through a requirement to repair or replace stolen, damaged or destroyed property.
Reputational damage	The reputation of Watercare being reduced in the eyes of stakeholders and/or customers, including a loss in confidence in Watercare's ability to provide lifeline utilities. See also the Watercare Risk Management Framework.
Disruption to operations	A reduction in the ability of Watercare to provide water or wastewater services. See also the Watercare Risk Management Framework.
Loss of information	Theft or destruction of sensitive Watercare information, including commercially, operationally or personally sensitive information, either belonging to Watercare or belonging to a third party and provided to Watercare with an expectation of privacy.
Harm to staff or other site occupants	Bodily harm to Watercare staff, contractors, customers or members of the public on Watercare property.

THREAT ACTOR

Petty criminal	A person using low sophistication, or no, tools in minimally planned or opportunistic criminal activity. Examples may include bored youths graffitiing a building or intoxicated persons stealing unsecured tools.
Motivated criminal	A person using moderately sophisticated tools and techniques, able to defeat basic security measures in potentially planned criminal activity. Examples may include a criminal gang targeting a Watercare site to steal valuable items such as computer equipment, with the ability to defeat perimeter fencing, force low-security doors and disguise their identity from CCTV cameras.
Insider	A person who has legitimate access to a Watercare site, including staff, contractors and authorised visitors. Insiders include those who use their legitimate access to target areas they are not authorised to access. Examples may include a maintenance contractor stealing items from a store they regularly access for their duties, or a front office staff member tailgating another staff member through an access-controlled door into an operational area they are not authorised to enter.
Activist	Someone who campaigns to bring about political or social change. In the context of this standard, an activist is someone who's campaign brings them into disagreement with Watercare and they take physical action in support of their cause. Examples may include protest activity at a Watercare site that blocks access points, denying Watercare staff, contractors and visitors access to the site.
Terrorist	Someone who is willing to threaten or use violence in pursuit of political or ideological aims. Examples may include someone introducing contamination into the drinking water supply with the aim of causing mass casualties or widespread panic, or someone who uses an explosive device to seriously disrupt Watercare operations with the aim of denying people lifeline utilities.
ADP	Fixated or Acutely Disaffected Persons are individuals who have an obsessional pre-occupation with a person, place or cause which is pursued to an irrational degree. Examples may include customers who become aggressive or violent as they have an issue with the cost of Watercare services, or a neighbour annoyed with the smell from a malfunctioning wastewater pump station who takes that frustration out on Watercare maintenance staff.

Appendix D – Watercare Specific Business Impact Levels

Table 8 contains a description of the PSR Business Impact Levels (BIL), tailored for specific relevance to Watercare.

Table 8 - Watercare-specific BILs.

LOW	MEDIUM	HIGH	VERY HIGH	EXTREME	CATASTROPHIC
Could be expected to impact Watercare operations by:	Could be expected to impede Watercare operations by:	Could be expected to affect Watercare operations by:	Could be expected to harm Watercare operations by:	Could be expected to have a major impact on Watercare operations by:	Could be expected to have a severe impact on Watercare operations by:
<ul style="list-style-type: none"> Causing degradation in organisational capability to an extent and duration that, while Watercare can perform its primary functions, the effectiveness of the functions is noticeably, though temporarily, reduced. Potentially adversely affecting a person's privacy. Resulting in minor damages to Watercare assets. Resulting in minor financial loss to Watercare that can be accommodated within existing budgets. 	<ul style="list-style-type: none"> Resulting in damage to Watercare assets. Resulting in moderate (up to \$1m) financial loss to Watercare. Resulting in minor, localised, adverse media coverage. Resulting in an internal investigation or inquiry. Resulting in some credibility issues within internal and inter-agency stakeholders. Resulting in minor harm to staff and/or members of the public. 	<ul style="list-style-type: none"> Causing moderate degradation in, or loss of, organisational capability to an extent that the Watercare cannot perform one or more of its primary functions for an extended period. Resulting in major damage to Watercare assets. Resulting in major financial loss (up to \$5 million). Resulting in adverse national media coverage. Significantly impacting on stakeholder relationships. Potentially harming some lives, though lives are unlikely to be lost. 	<ul style="list-style-type: none"> Causing a severe degradation in, or loss of, organisational capability to an extent that Watercare cannot perform some primary functions on an ongoing basis. Resulting in significant disruption to Watercare lifeline services. Resulting in significant financial loss (up to \$10 million). Sustained adverse national and international media coverage. Resulting in moderate environmental consequences. 	<ul style="list-style-type: none"> Causing a loss of organisational capability to an extent and duration that Watercare cannot perform any of its functions. Resulting in severe financial loss (over \$10 million). Resulting in serious harm to staff or the public, including loss of life. Resulting in major environmental costs. 	<ul style="list-style-type: none"> Leading directly to widespread loss of life. Causing severe long term damage to significant Watercare infrastructure. Leading to a long term and severe effect on the national economy. Having extreme and irreversible environmental costs.

Appendix E – Guidance on Setting Risk Levels

1. The process to evaluate risk levels is explained in the Watercare Risk Management Framework, but is summarised below in the context of physical security risks. It should be noted that the high, medium and low ratings used in this standard are designed to inform the level of physical security control measures required for a site and are not directly comparable to the rating contained in the Watercare Framework.
2. Risk consists of likelihood and consequence, with the risk rating the combination of these factors. Likelihood ratings, with examples, are shown in Table 9. Consequence ratings, with examples, are shown in Table 10. The resultant Physical Security Risk Rating is shown in Table 11, with red representing high risk, orange representing medium risk and green representing low risk. To determine what security controls are applicable, risk ratings should be determined in the absence of controls. If desired, the process can then be repeated after the application of controls to determine a residual risk rating.

Table 9 – Likelihood ratings

LIKELIHOOD RATING	DESCRIPTION	EXAMPLE
Very Low (1)	May occur on very rare occasions, but is not expected to occur.	Contamination of the fresh water supply causing a degradation in water quality caused by an issues motivated person or organisation.
Low (2)	Occurs, or is expected to occur, rarely.	Intentional harm to a staff member causing non-minor injuries. May occur once every couple of years.
Medium (3)	Occurs, or is expected to occur, occasionally.	Theft of expensive machinery or valuable materials, may occur once or twice a year.
High (4)	Occurs, or is expected to occur, frequently.	Vandalism to a site in a high crime area, may occur monthly.
Very High (5)	Occurs, or is expected to occur, very frequently.	Graffiti on fences that reappears within days of being cleaned.

Table 10 – Consequence ratings

CONSEQUENCE RATING	DESCRIPTION	EXAMPLES ⁶
Very Low (1)	Minimal impact	Unplanned loss of supply/service for less than 10 customers for more than 24 hours. Unconfirmed non-notifiable illness without a clear link to the water supply or wastewater discharges. Single community complaint to Watercare.

⁶ Consequence rating examples taken directly from the Watercare Risk Management Framework, Sept 2018.

Low (2)	Minor impact.	<p>Unplanned loss of supply/service for 10 to 100 customers for more than 24 hours</p> <p>Single person with non-notifiable illness with confirmed links to the water supply or wastewater discharges</p> <p>Complaints to regulators by interest groups.</p>
Medium (3)	Moderate impact.	<p>Unplanned loss of supply/service for 100 to 1,000 customers for more than 24 hours</p> <p>Multiple people suffer non-notifiable illness with a confirmed link to the water supply or wastewater discharges.</p> <p>One adverse local media/social media article highlighting community concern coupled with complaints to regulators by interest groups.</p>
High (4)	Major impact.	<p>Unplanned loss of supply/service for 500 to 1,000 customers for more than 24 hours</p> <p>Single person suffers notifiable illness with a confirmed link to the water supply or wastewater discharges.</p> <p>Continuing adverse local/social media coverage for less than a week expressing community concern coupled with pressure by political or other interest groups.</p>
Very High (5)	Significant impact.	<p>Unplanned loss of supply/service for 1,000 to 5,000 customers for more than 24 hours</p> <p>Multiple people suffer notifiable / serious disease with a confirmed link to the water supply or wastewater discharges.</p> <p>Continuing adverse local/social media coverage over weeks expressing significant community concern coupled with continuing pressure by political or other interest groups.</p>

Table 11 – Physical Security Risk Rating

LIKELIHOOD	V	5	10	15	20	25
	H	4	8	12	16	20
	M	3	6	9	12	15
	L	2	4	6	8	10
	V L	1	2	3	4	5
		VL	L	M	H	VH
CONSEQUENCE						
Risk rating:		High	Medium	Low		

Appendix F – Example Alert Level System

1. An alert level system enables the security configuration of a site to adapt to a changing threat environment. It should be underpinned by standard operating procedures that explain what actions are to be taken or measures put in place for each alert level, the procedure for raising or lowering the alert level, the authority to raise or lower an alert level and a process for ensuring all staff know what the alert level is and what they have to do in response.
2. Table 12 contains an example of a very basic alert level system for a site, based on the threat levels in Appendix B.

Table 12 – Example alert level system

ALERT LEVEL	DEFINITION	EXAMPLE EVENTS	EXAMPLE ACTIONS/MEASURES
Extreme	A security incident impacting Watercare, its assets, information or personnel, is expected or is occurring. This alert level imposes significant business impact and cannot be maintained for any length of time.	Protest activity that is expected to become violent is planned or is occurring at a Watercare site. There is an active shooter alert or incident at a Watercare site. There is a terrorism threat directed to a specific Watercare site.	No visitors or on site. Only operationally essential staff on site. Full time security presence on site. No deliveries accepted. All access points mechanically locked with security presence, positive ID required for entry. Police regularly updated, with a presence on site as required.
High	A security incident impacting Watercare, its assets, information or personnel, is assessed as highly likely. This alert level imposes moderate business impact and can be maintained for a number of hours.	Protest activity that has the potential to become violent is planned at a Watercare site. An armed or violent criminal offender is being actively pursued by Police near a Watercare site. A suspicious package or mail item is delivered. There is assessed to be a terrorism threat specific to NZ CNI or a non-specific water utility site.	No visitors or non-essential contractors on site. Staff work from home where possible. Increased frequency of security patrols, consider 24/7 security presence on site. EACS set to require dual authentication for all external access points. Only operationally essential deliveries accepted. Police advised and updated as required.
Medium	A security incident impacting Watercare, its assets, information or personnel, is assessed	Protest activity at a Watercare site is	No non-essential visitors or contractors on site.

	as a feasible and could well. This alert level imposes moderate inconvenience and some business impact, and can be maintained for a number of days.	planned. Violence is possible not expected. A spike in criminal activity is reported around the site area. The national terrorism threat level is increased, but no specific threat is known.	Staff work from home where possible. Increased frequency of security patrols. Increased screening of deliveries.
Low	A security incident impacting Watercare, its assets, information or personnel, is assessed as a realistic possibility. This alert level potentially imposes some minor inconvenience and business impact, and can be maintained for long periods.	Heightened community tension but no specific threat to Watercare sites or assets is known.	Security awareness communication to staff is increased. Baseline security control measures are reviewed more regularly and adjusted as necessary.
Very Low	A security incident impacting Watercare, its assets, information or personnel, is assessed as unlikely. This alert level can be maintained indefinitely.	Business as usual.	Normal baseline security control measures are in place.

Appendix G – Pump Station Baseline Controls

1. A set of baseline controls for pump stations, intended to be used as a starting point for routine pump station build projects, is detailed in the table below. Should any deviations from this baseline be required, and for any other site type, the security team must be consulted.
2. This appendix contains only basic control information and should be read in conjunction with the main standards descriptions in Section 4.

SECURITY CULTURE AND TRAINING	All staff, contractors and consultants must undertake training on the purpose and operation of security control measures (e.g. IDS) employed at sites where they have unescorted access.
SECURITY COMMUNICATION	Signage visible from the perimeter or beyond the perimeter, such as site maps or hazard boards, should not indicate the presence or location of critical, sensitive, high value or attractive items or areas.
SIGNAGE	Restricted access signs, including CCTV warning signs as appropriate, must be displayed at all access points and at other appropriate points around the site perimeter.
	Signs must state the area beyond the fence/gate/door is a restricted place and indicate the consequences of unauthorised access. ⁷
PERIMETER FENCING	The perimeter fence must be chain link with steel poles, including top and bottom rails OR concrete OR concrete block OR steel palisade.
	It must be a minimum of 1.8 m high and topped with three strands of barbed wire and flat coils of razor wire OR a minimum of 2.2 m high topped with steel spikes.
	It must incorporate fence sensors OR be backed with zoned monitored pulse electric fence ⁸ .
	Building exterior walls can form some, or all, of a site perimeter, but care must be taken to avoid potential climbing aids.
	Anti-climb measures (barbed/razor wire) should be used on single storied buildings where climbing could provide site access.
	A zone of 3 m (ideal) or 1.5 m (where appropriate) on either side of perimeter fence must be kept clear of vegetation or structures that could be used as climbing aids or surveillance blind spots.

⁷ Standard design security signage is available from the Watercare Security Team.

⁸ **Consider** de-energising or applying low voltage to the electric fence when the site is occupied.

SITE ACCESS POINTS	Perimeter access points must provide at least the same level of security protection as the remaining perimeter security measures that contain them.
	The number of access points in a site perimeter should be kept to a minimum with consideration to operational and potential evacuation requirements.
	Vehicle and pedestrian access gates must be constructed to the same or higher standard as the fence that contains them.
	Primary access points should be a manual swing or sliding gate secured with a padlock.
SITE APPEARANCE AND MAINTENANCE	All sites should be configured to reduce the opportunities for vandalism (for instance graffiti) by avoiding solid fencing where possible (concrete, wooden pale) and using building styles that deter graffiti.
	The site should be regularly maintained to give an impression of control, order and a sense of care and ownership.
FRESH WATER AND WET WELL DOORS AND HATCHES	All access points that provide access to drinking water (e.g. reservoir inspection hatches) or raw sewage (e.g. doors to wet wells) must be fitted with sensors (e.g. reed switch) that provide an alert to the Nerve Centre when they are opened.
	All access points must be physically secured. The minimum is a non-standard fitting (such as a Crox bolt).
	Access points that are publicly accessible must be secured with a mechanical lock, with preference given to keyed locks in doors or a steel bar laid over the centre of the hatch cover secured in place with a padlock.
BUILDING BOUNDARY CONSTRUCTION	Pump station buildings should be constructed to resist intrusion.
	Walls should be constructed to a high-quality commercial standard and maintained to that level.
	External windows should be avoided where possible.
	External windows should have steel security bars or grills installed.
	External windows should have privacy film installed.
	Any opening window should be permanently fixed closed or fitted with a window stay and keyed window lock.
	Windows at high risk of vandalism, such as those immediately accessible to public spaces, should be laminated glass or have anti-shatter film applied.
DOORS	External doors must be resistant to intrusion and be fitted with heavy duty two or three stage automatic door closers.

	External doors must be minimum 38 mm solid core wooden doors (or equivalent) hung on three or four evenly spaced fixed/captured pin hinges in steel (preferred) or solid wood frames.
	Doors must be outwards opening unless they are required to be inwards opening for fire escape/evacuation purposes.
	External outward opening doors should be fitted with three evenly spaced hinge bolts.
LOCKS AND ACCESS CONTROL	Perimeter access points should be integrated into the site EACS using electronic mortice or magnetic locks.
	Dual authentication (swipe and PIN) should be required for entry with swipe to exit.
	Access must only be provided to staff and contractors on a strict need-to-access basis.
	Door-open-too-long alarms should be enabled with local audible alarms, along with alerts at the Nerve Centre.
	Forced door and emergency door release should be enabled with local audible alarms and trigger alerts at the Nerve Centre.
	External pump station access points must be secured with mechanical deadbolt or padlocks after-hours using a restricted profile key within the Watercare key management system.
	The primary leaf of two-leaf doors must meet the requirements above with the secondary leaf being mechanically locked any time it is not in use using flush and/or door bolts. Secondary leaf mechanical locks must not be accessible without access first being granted through the primary leaf.
	Roller doors must be secured internally with tower bolts or similar and secured with a padlock.
CCTV	Consider CCTV coverage of access points to pump stations.
SECURITY LIGHTING	Security lighting must compliment CCTV cameras where applicable.
	Where possible, security lighting should be located within the site perimeter and at a sufficient height to reduce the risk of vandalism.
	Motion activated LED lights should be used where possible to reduce energy consumption and light pollution to neighbouring properties. Where motion activation is not practical or appropriate, timed switches should be used, or manually switched if this is the only practical option
	Security lighting must fully illuminate the primary perimeter access points and approaches which may be used after hours.
	Security lights should illuminate areas of the perimeter easily accessible to the public.

	Security lighting should provide general illumination to the full site.
	Building access points that might be used during the hours of darkness must be illuminated by security lighting.
	Consider illuminating the full perimeter of buildings.
IDS	Pump station buildings must be protected by an Intruder Detection System (IDS).
	Pump station buildings must be armed when unoccupied.
	The IDS must monitor all external doors to the building, including roller doors, through both volumetric movement sensors (PIR) and break surface door sensors (reed switch).
	Full area volumetric movement sensors should be installed.
	All IDS panels, keypads and sensors (PIRs, reed switches) must have tamper switches installed.
	Tamper switches must be configured to the system zone and require an administrator access to disable or bypass.
	Tamper switches must provide an alert at the monitoring centre when triggered, even when the IDS zone is unarmed.
	The IDS panel for the building must be within the building and covered by IDS sensors.
	The IDS control panel should be located in the most secure area of the building.
	The keypad to arm and disarm an IDS zone must be covered by the zone IDS sensors.
	The IDS must require two-factor authentication (swipe and PIN) to disarm.
	The IDS should require two-factor authentication (swipe and PIN) to arm.
	The IDS must be monitored 24/7.
	The IDS should be monitored by the Nerve Centre.
EACS	All EACS card readers, keypads and locking devices (magnetic and mortice locks) must have tamper monitoring installed.
	Tamper detection should be monitored by the Nerve Centre.
	EACS door locks must fail safe on the internal/secure side of the door.
	EACS door locks should fail secure on the external/insecure side of the door.

SSP	All sites must have a SSP.
	SSPs should be informed by, and complimentary to, the wider suite of Watercare security documentation.
	A site-specific threat assessment and security risk register should be included in the SSP.
	The SSP must include processes to respond to a heightened threat environment, including changes to physical security measures that may need to be implemented in the event of a pending or in-progress security incident. An example of a basic Alert Level system is included in Appendix F.
	SSPs must be reviewed at least annually to ensure they remain fit for purpose.
SECURITY COMMUNICATIONS NETWORK	All sites must have security communications network connectivity.
	Sites should have a connection to the Watercare corporate network infrastructure as the preferred transport medium for security communications.
	Remote viewing of CCTV footage requires significantly more network bandwidth than basic security system monitoring alone. Sites with CCTV must consider bandwidth when provisioning network connectivity.
	Watercare Digital must be consulted when planning and implementing security communications into the corporate network to ensure current network standards are met.
ELECTRONIC SECURITY CABINETS	All sites must have provision for a wall-mounted security cabinet with an associated mains power outlet.
	The security cabinet must be in an area protected by an IDS.
	The security cabinet should be located in the most secure area of the site.
	The security cabinet power should be connected to the site Uninterrupted Power Supply (UPS) and/or backup power, if available.
	The Watercare preferred security integrator must be consulted on security cabinet and power requirements during the design phase of significant site developments or new builds.
SECURITY CABLING	All security cables must be supported (e.g. catenary wire, cable trays or conduit).
	Security cables must be separated from mains power cable by at least 300 mm.