South East Water

healthy water for life

Water & Sewerage

Facility Security

AM2759

Contents

Document History

Version No.	Date	Author	Version Description
0	*Mar 2018*	*R. Jagger*	*Draft for Review*
1.0	*June 2018*	*R. Jagger*	*First Revision*

1. INTRODUCTION

1.1. Purpose of Specification

The purposed of this specification is to protect:

1) the safety of workers on site by preventing the entry of intruders who may directly (through violence) or indirectly (through creation of hazards) pose a threat,
2) members of the public from exposure to hazards at SEW facilities,
3) facilities from damage and any financial losses which would result, and
4) the function of facilities to ensure they can continue to meet their operational objectives (ie: safe and reliable water supply and no unlicensed discharges to the environment).

This specification is to be used by SEW staff and contractors that design, construct, operate, maintain and manage SEW owned facilities. This specification follows the structure and principles documented in AS HB 167- Security Risk Management.

1.2. Scope of Specification

This specification is to apply to all water and sewerage facilities but excludes the main SEW office building at WaterEdge and maintenance depots not located at Treatment Plants. Facilities are deemed to be operational sites that contain mechanical or electrical equipment, including small facilities that may only contain air treatment canisters and flow meters etc. Sites which only contain civil pipeline assets are not considered to be facilities.

While this specification may over time be applied to existing facilities, its main objective is to document the requirements for all new facilities and those being substantially upgraded or renewed.

1.3. Key References

The following key references provide further information relevant to this specification:

- Australian Standard for Security Risk Management. HB 167: 2006
- Australian Standard for Chain link fabric fencing- Part 1. AS 1725.1: 2010
- AS 3559 – Buildings in Fire Prone Areas
- Security Vulnerability – Risk Assessment Guideline (SV-RAG) for the Victoria Water Industry
- SEW Bush Fire Management Plan
- SEW Terrorism Risk Management Plan, BS 1869
- SEW Incident Management Plan, BS 1868
- SEW Business Continuity Plans
- SEW Lock and Key Procedure (under development)
- SEW Electronic Surveillance Specification (under development)
- SEW Asset Entry Procedure, AM2426 (network facility access only)
- SEW Electrical and Data Specification, AM2714
- SEW's Specification for Covers of Underground Structures, AM2756
- Preventing graffiti and vandalism. Australian Institute of Criminology- 1996.

2. CONTEXT AND THREATS

SEW is located in a prosperous city and country which (relative to the world in general) has:

- A low and stable crime rate
- Stable and functional government

- Well-resourced and effective police, intelligence and judicial systems
- Few examples of effective terrorist actions
- Low unemployment and disadvantage (although there is substantial variety in this).
- Moderate levels of natural disaster, although bushfire and floods are fairly common.

The below threat assessment is based on this context remaining in place. Should climatic, social, political or economic factors change significantly, the threats which apply to water and sewerage facilities ought to be reassessed.

The threats facing our water and sewerage facilities can be summarised as follows:

Table 1: Threats Facing Water and Sewerage Facilities

Threat	Group	Capability	Intent	Australian Precedence
Malicious Damage	Terrorists	Moderate	High	None known
Malicious Damage	Vandals or Arsonists	Low	Low	Common
Malicious Assault on Workers	Aggrieved or Violent Residents	Low	Low	Rare
Incidental Damage	Vehicle Drivers	Low	Low	Rare
Incidental Damage	Falling trees / limbs	Low	Low	Occasional
Incidental Damage	Bushfires, Flood & Storms	High	Low	Occasional
Incidental Damage	Livestock	Low	Low	Rare

Notes regarding Table 1:

- Capability refers to the means available to the group to cause widespread injury or damage.
- Intent refers to the level of determination and planning likely to be deployed by the group.

2.1. General Response to Malicious Threats

The ability of SEW to prevent terrorist threats is difficult because:

- The capability and intent of terrorists is likely to be moderate or high.
- The timing of any incident is unpredictable.
- The practicality of preventing access to determined groups is low given the number, size and spread of the facilities we are trying to protect.

SEW is somewhat reliant on government agencies to prevent malicious threats through their law enforcement activities. These activities include gathering intelligence and prosecuting potential offenders to reduce the security risk.

The optimum strategy for SEW to deal with malicious threats is to:

1) Implement basic preventative measures to discourage access by groups with low intent and low capability (eg: children and opportunistic offenders).
2) Detect intrusion when it occurs so that we can respond rapidly.
3) Respond appropriately to the intrusion once it occurs.

2.2. General Response to Incidental Threats

The optimum strategy for dealing with vegetation risks, bushfire, flood, storms and livestock risks is to assess the risk of such events and put in place risk controls such as suitable physical enclosures, backup power, elevation above the flood level and removal of vegetation.

Where the vehicle damage risk is significant, this risk should in most cases be prevented through the installation of physical obstructions.

3. MALICIOUS THREATS

The malicious threat to a facility should be assessed in accordance with the **Security Vulnerability Risk Assessment Guideline for the Victorian Water Industry**. Malicious threats shall be determined on the basis of Likelihood (Threat) x Consequence (Harm) in consideration of the below factors.

3.1. Likelihood (Threat)

The likelihood of malicious security risks to water and sewerage facilities should be assessed in consideration of the following risk factors:

- Historical precedence of vandalism (particularly relevant to existing facilities)
- Historical precedence of unauthorised access (particularly relevant to existing facilities)
- Prominence of the facility. Facilities which fit in with or do not look out of place in their environment are less likely to attract the attention of malicious groups.
- Evidence of neglect or abuse of public infrastructure evident (eg: bus shelters, park benches, public toilets etc)
- Neighbourhood poorly lit (ie: limited or no street or park lighting)
- Low exposure of facility to local residents (ie: facility is distant from houses or high use public spaces)
- Low exposure of facility to night time traffic
- Security measures in place.

It is assumed that areas that receive regular public scrutiny are less likely to be illegally entered as potential offenders would be deterred from undertaking such actions in front of witnesses.

“Damage breeds more damage” describes the effect that poor asset condition and neglect has on increasing the amount of further wilful damage. Inspecting facilities and maintaining them in good condition is one way of reducing the likelihood of malicious threats.

3.2. Consequence (Harm)

The consequence of malicious security risks to water and sewerage facilities should be assessed in consideration of the following risk factors:

- The risk to water quality and human health
- The risk to the environment from inadequate plant performance
- The degree of risks and hazards present at the facility
- The size of the facility and the size of its output
- The amount of plant typically contained at the facility
- The exposure of plant to easy above ground access

A minimum risk level of Medium should be applied to treatment plants and drinking water storages as it is considered prudent to have some form of electronic surveillance at all of these facilities.

3.3. Malicious Threat Controls

The optimum risk controls for a facility should match the type and magnitude of the threats identified.

Measures may be selected to include:

1) Deter and delay incidents (refer Table 2 items 1, 2, 4, 8, 10)
2) Detect incidents (refer Table 2 items 2, 3, 5, 6, 9, 10)
3) Respond and recover from incidents (refer Table 2 items 7, 8, 9, 10, section 6 of this report)

Table 2: Malicious Threat Risk Control Options and Recommendations

ID	Risk Control Description	Relevant Security Levels
1	Plant and equipment contained within locked buildings, cubicles, tanks or chambers	All facilities
2	Facility access registration or monitoring	All facilities
3	Gate, door and hatch position switches and alarms	All facilities
4	Security fencing and locked gates	Low or Medium +
5	Intruder detection (eg: beams, infrared, microwave)	Medium +
6	CCTV monitoring	Medium +
7	Detector activated flood lighting	Medium +
8	Scheduled Inspections	Medium +
9	Loudspeakers (for alarm &/or voice)	High +
10	Mobile security patrols (outside working hrs)	High +

The lowest order risk control will typically apply to all facilities and the highest security risk facilities may require all risk controls. Table 2 is a guide only. The practicality and individual design of each risk control will need to be assessed for each facility on a case by case basis, using the principals and issues described in the following sections.

4. INCIDENTAL THREATS

Incidental threats are those which are not malicious (intentional).

4.1. Incidental Threat Assessment

Each of the threats described in Table 3 should be evaluated for each facility and a security level assigned for each threat. Low can be considered to represent the lowest risk amongst the same cohort of SEW facilities and High can be considered to represent the highest risk amongst the same cohort of SEW facilities. For example, a facility located 100m down a SEW owned driveway represents a Low vehicle strike risk level. One located immediately adjacent to a 3 lane inner city major road represents a High vehicle strike risk level.

Table 3: Incidental security risks, their assessment and controls

Security Risk	Assessment criteria	Risk Level Range	Potential Controls
Falling limbs / trees	How likely are trees / limbs to fall and what would be the consequence if one did. Depends on size, species, age, condition and location of vegetation.	Low	Regular arborist assessment of risk. Remove or prune high risk vegetation.
Flood	Elevation of asset relative to flood level. Sensitivity of the assets to water damage. Access to site during floods.	Low – High	Elevate assets. Levy banks. Relocate assets to higher ground. House assets within submersion proof enclosures.
Vehicle strike	Proximity of asset(s) to traffic. Sensitivity of assets to collision. Existing barriers protecting assets.	Low – High	Locate assets away from road(s). Install barriers to prevent collision (trees, bollards, railings).

	Degree of traffic and traffic speed on adjacent road(s).		House items within a building.
Storms (wind & lightening causing power outage)	Reliance on power supply (can facility operate on DC or backup power). Reliability of mains power supply (dual feeds to power zone). Level of isolation of the facility.	Low - High	Additional storage of water / sewage. Implementation of backup power.
Livestock (trampling fences / assets	Presence of livestock adjacent to the facility. Size and number of animals	Low	Consider installing a farm fence to prevent livestock damage. Protect items to restrict damage due to trampling should livestock gain access.
Bushfire	Refer section 4.3		

4.2. Incidental Threat Controls

The optimum risk controls for a facility should best match the type and magnitude of the threats identified.

Measures may be selected to:

1) Deter and delay incidents (refer Table 4 items 1, 4, 11, 12, 13, 14, 15 & 16)
2) Detect incidents (refer Table 4 items 6, 9)
3) Respond and recover from incidents (refer Table 4 item 8, 9, section 6 of this report)

Table 4: Incidental Risk Control Options and Recommendations

ID	Risk Control Description	Relevant Threat
1	Plant and equipment contained within locked buildings, cubicles, tanks, chambers or housing.	Falling trees. Bushfire. Flood. Vehicle Strike. Livestock
4	Security fencing and locked gates	Vehicle Strike. Livestock
6	CCTV monitoring (can monitor what is happening without needing to put personnel at risk undertaking surveillance)	Falling trees. Bushfire. Flood. Vehicle Strike. Livestock.
8	Scheduled Inspections	Falling trees. Bushfire. Flood. Vehicle Strike. Livestock.
10	Mobile security patrols (outside working hrs)	Falling trees. Bushfire. Flood. Vehicle Strike. Livestock.
11	Facility Location and Set Out of Assets within Facilities	Falling trees. Bushfire. Flood. Vehicle Strike.
12	Vegetation Management	Falling trees. Bushfire.
13	Bollards and barriers	Vehicle Strike
14	Water / sewage storage	Storms – Power Outages
15	Backup power	Storms – Power Outages
16	Farm fencing	Livestock

Table 4 provides the security control measures which may be deployed for facilities of different incidental security risks. The lowest order risk controls may apply to all facilities and the highest security risk facilities may require all risk controls. Table 4 is a guide only. The practicality and individual design of each risk control will need to be assessed for each facility on a case by case

basis, using the principals and issues described in the following sections. Where the risk is Low, it may be appropriate not to implement any controls.

4.3. Bushfire Risk Management

Bushfire risk for new facilities shall be assessed as follows:

1) Determine if the facility is in a high Bushfire risk area (refer below).
2) If it is, assess (or engage a fire safety consultant to assess) the BAL rating in accordance with AS 3559 (most recent edition) for different potential asset locations at the site.
3) Locate assets at the site to minimise the BAL rating of the asset as much as practical.
4) Consider and implement options to reduce the BAL rating where it is reasonable and cost effective to do so (eg: clear vegetation near the asset).
5) Design asset enclosures and buildings depending on the final BAL rating in accordance with AS 3559 (refer section 5.3- Physical Protection of Assets)

High bushfire risk areas are indicated in Figure 1 and include:

- Arthurs Seat & McCrae
- Beaconsfield Upper
- Belgrave, Belgrave South & Belgrave Heights
- Blairgowrie & Sorrento
- Cannons Creek
- Cape Shank & Portsea
- Ferntree Gully & Upper Ferntree Gully
- Fingal & Tootgarook
- Harkaway
- Lysterfield & Lysterfield South
- Mount Martha
- Nar Nar Goon North, Tynong North & Garfield North
- Pakenham Upper
- Rosebud
- Rowville
- Selby &Tecoma
- St Andrew's Beach & Rye
- The Basin
- Upwey
- Warneet and Blind Bight

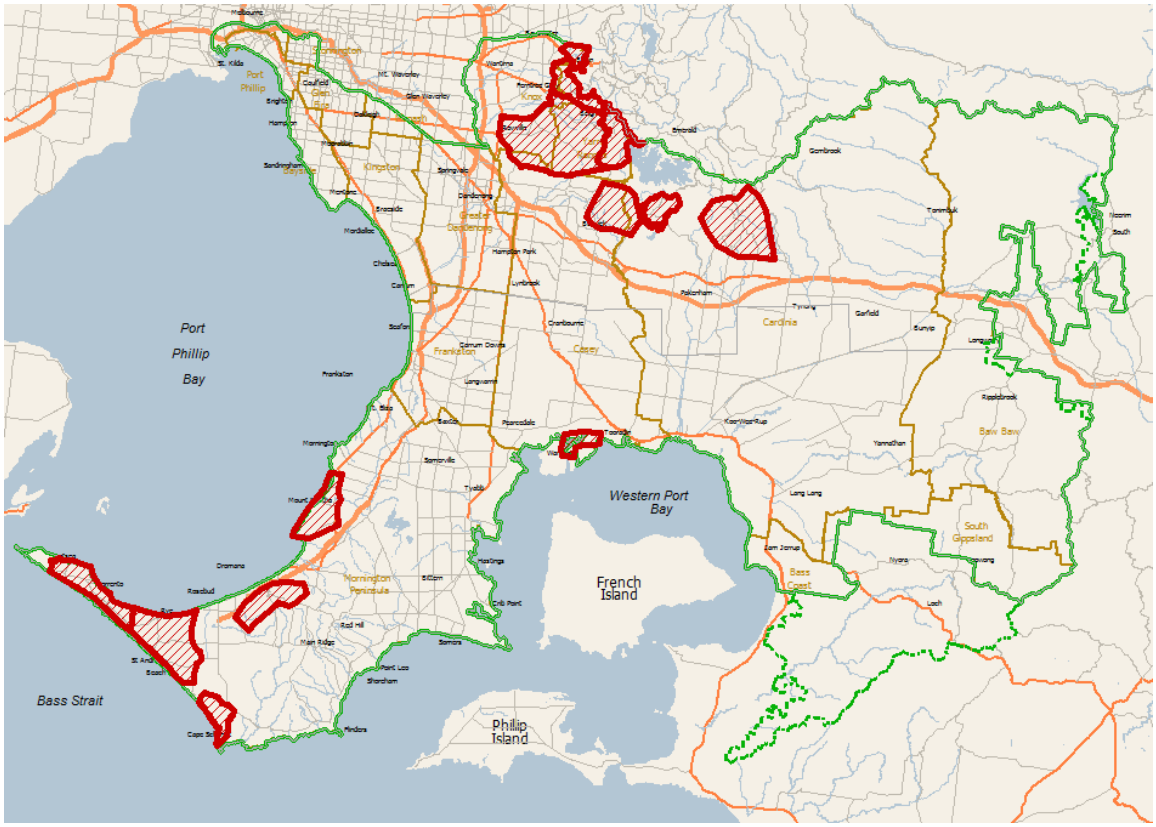

Figure 1: High Bushfire Risk Areas in South East Waters Region

Detailed plans indicating the exact boundaries of these areas are available in SEW's Bushfire Management Plan.

AS 3959 demonstrates two methods for determining the Bushfire Attach Level (BAL) which are as follows:

- Method 1 – a simplified procedure to determine the BAL; &,
- Method 2 – a detailed procedure using calculations to determine the BAL where a more specific result is sought or where the site conditions are outside the scope of the simplified method (Method 1).

Generally, the BAL may be determined using the simplified procedure (Method 1) which involves the following steps:

1. Determine the relevant Fire Danger Index (FDI).
2. Determine the vegetation types. The Standard provides guidance for the classification.
3. Determine the distance of the facility from the classified vegetation.
4. Determine the effective slope(s) under the classified vegetation adjacent to the site.
5. Determine the BAL from the appropriate table.

In BAL-FZ rated areas, consider installing a high quality deluge system that sprays the full area of the asset to significantly reduce the risk of embers and radiant heat damage to the assets. The deluge pressure system should not be solely reliant on a mains powered pressure pump for its operation. Ideally, it should be connected to a gravity pipeline/tank system or a sufficiently protected diesel type fire pump. Provided the deluge system continues to operate during a fire event, there is a much higher probability that the structure would survive, as has been demonstrated during recent bushfire events in Victoria.

5. SECURITY RISK CONTROL IMPLEMENTATION

5.1. Roles and Responsibilities

Security requirements and their implementation should be implemented as follows:

Table 5: Security Assessment and Implementation Responsibilities

Asset Status / Method of Delivery	Responsibility to Assess and Communicate Requirements	Responsibility to Implement Security Measures
Existing Operational Facilities	Customer Service Delivery	Customer Service Delivery
Operational Facilities due to be Renewed or Upgraded by SEW New Facilities to be constructed by SEW	• Customer Service Delivery shall document the requirements. • The SEW officer compiling the Project Brief shall include these requirements in the Tender / RFQ	• The engaged construction contractor shall implement the measures (possibly by engaging SEW approved suppliers or staff). • The SEW project manager shall provide oversight. • The correct functioning of all security measures shall be verified during the commissioning process.
New Facilities to be constructed by Developers	• Customer Service Delivery shall document the requirements. • Land Development shall include these requirements in Development Agreements.	• The developer (or delegate) shall implement the measures (sometimes by engaging SEW approved suppliers or staff). • The correct functioning of all security measures shall be verified during the commissioning process.

Notes regarding Table 5:

- The SEW personnel or contractors able of perform security works may be limited and/or controlled by Customer Service Delivery (eg: electronic surveillance may only be implemented by approved specialist contractors).
- Security requirements shall be documented in the Development Agreement / Tender / RFQ.
- External parties engaged to construct facilities shall implement the required security measures in accordance with these requirements at their cost.

5.2. Locks

The selection, attainment process and deployment of locks and the issuing and control of keys shall be undertaken in accordance with SEW's lock and key procedure (under development).

5.3. Facility Access Registration or Monitoring

The entry and exit of personnel to network facilities is controlled and recorded as per AM2426-Asset Entry Procedure. One of the purposes of this procedure is to enable personnel within the Network Operations Centre (NOC) to determine if Intruder Alarms have been triggered by intruders or legitimate operatives.

5.4. Physical Enclosure of Assets

All significant mechanical and electrical items shall be contained within locked buildings, cubicles, tanks or chambers where practical. This is especially important for high value (ie: > $5,000) or critical items (especially those that are essential to the operation of the facility). Housing important items in this way can protect them from:

- Malicious threats such as vandalism and terrorism.
  Locked enclosures hide items from view and ensure that only authorised or determined groups could access the items.
- Bushfire and arson.
  Housing assets within fire / heat resistant enclosures is one of the most effective way of preventing fire damage.
- Falling trees.
  Mechanical protection of assets may protect them against falling trees or limbs.
- Flood.
  Where practical, all non-submersion rated mechanical and electrical equipment should located above the 1 in 100 year flood level. When this is not practical, items below the flood level shall be protected by enclosing them in submersion proof housing which is IP58 or IP68.
- Livestock.
  Housing items within enclosures provides a level of protection from livestock that have gained entry to the facility.

It may not be appropriate for mechanical and electrical items to be protected this way (eg: actuators, instruments, cables and valves at treatment plants) and it may be more appropriate to rely on a fenced compound which has electronic surveillance to provide protection.

5.4.1. Underground Structure Covers

All underground chambers shall be covered as per SEW's Specification for Covers of Underground Structures, AM2757.

5.4.2. Tank Hatch and External Cubicle Requirements

Above ground tank or reservoir roof hatches and any facility external cubicles (those not contained within locked buildings) shall be designed and constructed in accordance with the appropriate Facility standards.

Where these are silent, hatches and external cubicles (cabinets) shall be constructed from welded or folded 3mm thick marine grade aluminium or stainless steel, powder coated Eucalyptus Green to AS2700, colour G52. Door hinges shall be Lenlok (chrome plated) or full length stainless steel continuous (piano) hinges with minimum 4.5mm diameter hinge pin(s). SEW standard locks shall be located at both unhinged door corners for added strength. Locks shall be shrouded to prevent the access of cutting tools.

Tank hatches shall be IP54 rated and external cubicles shall IP56 rated. All stainless steel components shall be in accordance with SEW's stainless steel specification, AM2760. External cubicles shall be located entirely above the 1 in 100 year flood level.

In high risk bushfire areas (refer figure 1), external cubicles shall be BAL rated, designed and constructed to comply with AS 3559.

5.4.3. Buildings and Enclosures

Where mechanical and electrical equipment cannot be effectively or sensibly housed in underground structures, tanks or external cubicles, it is typically best to locate these items in a building or enclosure. The building or enclosure should be designed to control the identified security risks on site.

Low risk facilities shall have buildings compliant to normal commercial building standards as per the Building Code of Australia. Additional requirements for higher risk buildings include:

- High malicious risk facility buildings shall have:
  a) Heavy duty construction in the form of double brick, stone or concrete walls.
  b) No Windows. If windows cannot be avoided for some reason, they shall be bared on the outside with 10mm thick steel bars at 100mm spacing.
  c) Doors shall be commercial grade heavy duty fully metallic doors with $\geq$ 2mm outer plate galvanised steel skin, 4 heavy duty SS hinges (with a pin diameter $\geq$ 4.5mm) and two heavy duty SEW approved locks, one near each unhinged corner.
- BAL-FZ rated assets generally require the following (ref AS 3559):
  a) Walls of non-combustible material (eg masonry, brick veneer, concrete) with a minimum thickness of 90mm or a system with a Fire Resistance Level FRL of 30/30/30 (30 minutes).
  b) Vents and weepholes in external walls shall be screened with a corrosion resistant steel or aluminium mesh with a maximum aperture of 2mm.
  c) Glazing shall be toughened glass minimum 5mm (all glazing including doors, windows, skylights).
  d) Where glazing is less than 400mm from the ground (including door glazing), that portion shall be screened with corrosion resistant steel or aluminium mesh or perforated sheet with a maximum aperture of 2mm. Alternatively, replace glazing with blockwork or other fire rated cement sheet.
  e) The openable portions of windows (flyscreens) shall be screened with a corrosion resistant steel or aluminium mesh with a maximum aperture size of 2mm.
  f) Doors shall be tight fitting all round and include weather strips and draught seals.
  g) The roof should consist of a system with a Fire Resistance Level FRL of 30/30/30. Note that standard Colorbond Steel roof sheet would not comply without an internal lining that has an FRL of 30/30/30 and that is fastened to the outside of the building structure.
  h) It must not have any gaps greater than 3mm under corrugations or ribs of sheeting or between roof components. Gaps shall be sealed at the fascia or wall line and at valleys, hips and edges by a 2mm steel/aluminium mesh, mineral wool and non-combustible material.
  i) All overhead glazing shall be Grade A laminated safety glass complying with AS 1288. Glazed elements in skylights may be polymer provided a Grade A safety glass diffuser, complying with AS 1288, is installed under the glazing. The skylights shall be protected with 2mm steel/aluminium ember guards.
  j) Fascias should be made of bushfire resistant timber or metal fixed at 450mm centres.
  k) Eaves linings should be 4.5mm min fibre cement sheet or bushfire resistant timber.
  l) Eaves penetrations shall be protected as per roof penetrations.
  m) Protect any above ground electrical/controls cabling and cabinets.

n) Seal all openings in the eaves and fascias with plastic moulding or fire resistant fibre cement sheet or sealant.
    i. Provide ember guards to intake and exhaust ventilation louvers.

- Medium and High flood risk buildings shall be built so that the floor is above the 1 in 100 year flood level, or a levy bank to the 1 in 100 year flood level shall be built around the full perimeter of the building.
- Buildings with a high tree / limb falling risk should be constructed of double brick, stone or concrete walls.

Buildings and commercial grade buildings in particular may not be acceptable to local residents, businesses or council. Consult with the local community as required to determine the level of acceptance for such assets. Where the intended building is not acceptable to locals, consider compromising on the height or appearance (consider what architectural beautification may be necessary). Also consider whether the building could be eliminated and other security measures (eg: bollards, tree removal, relocation) implemented instead.

5.5. Fencing and Gates

Security fences shall typically be located at the perimeter of the land parcel designated for the facility. On occasion, at larger facilities, it makes sense to have an external farm fence at the perimeter with an internal security fencing around the areas where assets are located.

Farm fences shall be as follows:

a) 90 or 100mm diameter treated pine posts at 4m spacing, inserted > 500mm below ground, protruding >1.2m above ground.
b) 2.5mm diameter high tensile heavy galvanised plain wire strands, each strand running through 3mm diameter post holes drilled centrally.
c) Fence to contain 6 wire strands and stand at a height of 1.2m above ground.
d) Bottom wire to be no more than 150mm above ground. All strands to be equispaced.
e) All strands to be tensioned to > 4kN.
f) Where livestock may exist on the other side of the farm fence, all wire strands shall be barbed wire.
g) Barbed wire shall be AS 2423 high tensile $\geq$1.57mm wire with a reverse twisted pattern construction and barbs at $\leq$100mm spacings, fastened to the outside of posts.

All facility above ground items (including open doors, gates and covers) shall be located a minimum of 1000mm away from fences and gates. To reduce the risk of damage to fences and gates, they should be located away from hanging branches and trees. Alternatively, vegetation within striking distance of fences should be removed where practical.

All low and medium risk security wire fencing and gates shall be designed and constructed in accordance with AS 1725.1 - Security fences and gates- General requirements. The fence types and options from this standard shall be adopted as per table 6.

Table 6: Fence and Gate requirements

Risk Level	Fabric Height	Fabric Wire		Pipe Grade	Standard
Low	2.1 m	2.5mm wire	Wire shall be with zinc-aluminium alloy coated within 1km of the coast. Otherwise, coat wire with galvanised zinc.	≥ DN50 Class 1 (posts). ≥ DN40 Class 1 (rails)	AS 1725.1, Type 2--T-B/B-T. (Rail top and bottom with 3 strands barbed wire. Cranked top). 4000 wide gates required as per Figure K3 in Appendix K.
Medium	2.4 m	3.15mm wire			
High	2.4m high post fence with additional outwards curved top. 3mm thick sheet metal "W" shape pales and triple point spear top. All posts, rails, fasteners and fastening plates to hot dip galvanised to AS 4680.				Maxiguard (R) to BS 1722-12 2006 (supplied by Gryffin or approved alternative). Gate dimensions as above.

Fences, gates or barbed wire may not be acceptable to local residents, businesses or council. Consult with the local community as required to determine the level of acceptance for these assets. Where fences and gates are not acceptable, consider compromising on the height or appearance (black coating instead of metal coating) of the fence. Consider whether security fencing could be eliminated and other security measures (eg: housing of items) bolstered to compensate for not having a fence.

5.6. Electronic Surveillance (Intruder Detection and CCTV)

All external building doors, cubicle doors and tank hatches shall have position detection and intruder alarms configured as per the SEW Electrical Standards AM2714 and standard SEW PLC, RTU and SCADA configuration files.

Electronic surveillance devices shall be selected and configured in accordance with Customer Service Delivery requirements and SEW Electronic Surveillance standards (under development). The number, type, location and set up of electronic surveillance devices shall be decided upon in consideration of the risk level and risks identified. Typically, the higher the risk level, the greater the diversity and amount of electronic surveillance required. Table 7 provides guidance on appropriate electronic surveillance measures for different threats.

Table 7: Hierarchy of Electronic Surveillance

ID	Risk Control Description	Malicious Threat Level	Incidental Threat Level
A	Facility access registration or monitoring. Presently manual. May become automatic with number plate recognition.	Low +	NA
B	Gate, external door and hatch position switches and alarms	Low +	NA
C	Critical access point intruder detection alarm (PIR, ultrasonic, beam). Critical access points are typically at the top or bottom of ladders, landings or in front of prominent external doors.	Medium +	NA
D	Critical access point CCTV monitoring. CCTV cameras are typically set up to remotely view the area(s) where intruder detectors are set up.	Medium +	High
E	Perimeter intruder detection alarm (fence climb / fence cut detection, PIR, ultrasonic, beam)	High	NA
F	Perimeter CCTV monitoring or pan 360 deg monitoring of "whole of site"	High	High

The number, field of view or path of detection of detectors and CCTV cameras should take into account the following:

a) The risk level and size of the facility.
b) The optimum layers of detection. One of the more effective detection arrangements consists of a full perimeter detection plus inner ring(s) of detection around key areas.
c) Minimisation of false alarms (often triggered by animals or falling vegetation). Diversity of sensor types and configurations are often more effective (ie: multiple sensors of a different type need to simultaneously trip to trigger a control room alarm).
d) Availability and distance to a power supply and communications hub.
e) The location of trees and other structures which may block images or beams.
f) Opportunities to elevate cameras to extend their field of vision. Ideally CCTV cameras should be set up to view as much area (particularly higher risk areas) as possible.
g) Areas which are historically accessed by intruders.
h) The cost and types of detectors available at the time of implementation.
i) Variations in light and shade. Facilities subject to sudden changes in cloud cover (usually due to windy conditions) can lead to false alarms generated from image analysis detectors (which work off light flux)

5.7. Detector Activated Flood Lighting

Detectors may be set up to trigger any or all floodlights at the facility to be switched on for a period of time during the night time. Detectors subject to being falsely triggered may be unsuitable as a means switching this automatic lighting, especially in areas where neighbours may be affected by the light.

LED flood lighting shall be set up to provide occupational outdoor lighting in accordance with AS/NZS 1680.1 Interior and Workplace Lighting. Detectors may trigger this lighting or even lighting specifically established to provide enhanced security at the facility.

5.8. Mobile Security Patrols

Mobile security patrols have the following advantages:

- They can be quickly established where urgent security improvements are required (ie: during or after an incident or when the National Terrorism Threat level escalates).
- They can patrol and inspect the whole facility (there are no blind spots).
- They are armed and trained in dealing with threats. They can present a safer first response option than operations or maintenance staff where it is not appropriate to call the police.
- The timing of visits can be somewhat random and unpredictable to intruders.

Mobile security patrols have the following disadvantages:

- They only provide surveillance for a relatively small portion of time.
- They potentially expose workers to threats.
- There is no recorded image of historical events (ie: the quality and quantity of evidence available for investigations is less).

For these reasons, mobile security patrols should be arranged when:

- Temporary or urgent improvements to security are required.

- The facility has a significant number of blind spots that are not practical to monitor with electronic surveillance.
- A significant amount of the existing electronic surveillance is out of service.
- It is the most appropriate first response option (refer to section 6 for more information).

5.9. Facility Location & Set Out of Assets within Facilities

Both the selection of the location for a facility and then the location of assets within that facility should be selected in consideration of the following factors:

Table 8: Considerations Affecting Facility and Asset Location

Risk	Consideration	Optimum Outcome	Alternative Action(s)
Falling Limbs	Location of existing vegetation	Locate susceptible assets away from risky vegetation	Remove any risky vegetation. Install susceptible assets within solid impact proof housing.
Bushfire	BAL rating	Minimise BAL rating by selecting appropriate land and location	Ensure all items susceptible to fire damage are protected through appropriate design
Flood	Site elevation	Locate facility away from flood prone areas (above 1 in 100 year flood level)	Install mechanical & electrical assets: - on higher ground in the facility. - within a levy bank - on elevated structures. - in submersion proof housing.
Vehicle Strike	Location of nearby roads and degree of traffic	Locate facility away from busy roads	Set back impact susceptible assets away from the road. Install bollards or barricades to separate vehicles and assets. House impact susceptible assets within an impact proof structure.
Storms (wind, lightening, power outage)	Likelihood & severity of Storms and Power Outages	Locate facility away from areas with a history of storms and power outages	Install two power supplies from different zones in the grid. Install on-site backup power supply. Install additional water / sewage storage.

5.10. Vegitation Management

Vegetation can pose a number of security threats. It can:

- Increase the fuel loading at a facility and therefore increase the risk of fire damage.
  The risk depends on the risk of bushfire at the facility. Vegetation and in particular thick vegetation may need to be kept well clear of critical assets or those sensitive to heat. Where necessary, expert advice should be sought on the fire risk at a facility and how the risk can be better controlled through changes to vegetation.
- Provide a means for intruders to bypass security fences.
  Intruders may be able to climb a tree and drop over a fence to gain entry or egress. Vegetation which may grow tall enough and be close enough to fences to enable this should not be planted and should be removed if present.
- Screen electronic surveillance from monitoring areas within the facility.
  Any vegetation that unduly affects electronic surveillance should be reduced in size or removed.

- Lead to false electronic surveillance intruder detector alarms.
  Vegetation which has a tendency to drop limbs and branches should not be selected or located near areas monitored by motion affected detection devices (microwave or beam detectors).
- Screen intruders from being seen by members of the public that could otherwise report the intrusion.
  Any vegetation that restricts members of the public from observing intruders should be reconsidered. This vegetation may however, provide a valuable screen which improves local aesthetics.
- Fall over or drop limbs which may damage assets within the facility.
  Vegetation which has a tendency to drop limbs and branches or is in poor condition and may fall over should not be selected or located near areas containing assets that might be affected. An alternative to removing vegetation is to provide a greater degree of mechanical protection of the asset(s) via improved housing.

The size, type and location of vegetation should be considered and controlled to reduce these risks to an acceptable level. These risks need to be weighed up against the benefits that vegetation provide in terms of improved visual aesthetics and shading of the facility from the sun and heat.

5.11. Bollards and Barriers

Bollards and barriers should be applied at facilities to prevent:

- Members of the public from damaging assets by accidentally veering off the road and into or over assets or workers. Use “Standard Duty” bollards and barriers.
- Provide a demarcation and restraint to prevent SEW authorised vehicles from driving into or over assets or workers. Use “Standard Duty” bollards and barriers.
- Provide from malicious group vehicle strike protection for high criticality assets and workers. Use “Heavy Duty” bollards and barriers.

Vegetation or fencing may provide adequate vehicle strike protection in lieu of bollards or barriers.

Bollards and barriers shall be designed and installed as per AM2761, Facility Vehicle Access Specification.

6. RESPONSE TO SECURITY BREECHES

Refer to the Incident Management Quick Links directory to find SEW relevant procedures at:
http://sewintranet/Assets/Lists/Incident%20Management%20Quick%20Links/All.aspx

Documents of particular relevance to Security breeches include the following:

- BS1869- Terrorism Risk Management Plan
- AM1363- Network Services Incident Management Checklist
- AM1985- Water storage tank hatch response procedure
- AM1986- Water storage tank video security alarm response procedure
- SEW Bushfire Management Plan

7. APPENDIX A: PROJECT SPECIFICATION

The following risk and facility design and construction requirements shall be implemented as part of the project.
Instruction to SEW PM: Complete all blank cells in Table 1 in Consultation with Customer Service Delivery and place Appendix within the Brief to go to RFQ / tender. Delete instruction once task complete.

Table 1: Malicious Threats

Threat	Present Yes / No
Historical precedence of vandalism (particularly relevant to existing facilities) The level of security in place	
Historical precedence of unauthorised access (particularly relevant to existing facilities)	
Prominence of the facility. Facilities which fit in with or do not look out of place in their environment are less likely to be noticed by malicious groups.	
Evidence of neglect or abuse of public infrastructure evident (eg: bus shelters, park benches, public toilets etc)	
Neighbourhood poorly lit (ie: limited or no street or park lighting)	
Low exposure of facility to local residents (ie: facility is distant from houses or high use public spaces)	
Low exposure of facility to night time traffic	
Overall Threat Level (L / M / H)	

Instruction to SEW PM: Remove all unrequired controls (rows) from Table 2 & edit as required. Delete instruction once task complete.

Table 2: Malicious Threat Risk Controls to be Implemented

ID	Risk Control Description	Required Yes / No. Specification
1	Plant and equipment contained within locked buildings, cubicles, tanks or chambers	Y. All
2	Facility access registration or monitoring	*(Instruction to SEW PM. Specify any electronic facility entry monitoring required)*
3	Gate, door and hatch position switches and alarms	Y. All
4	Security fencing and locked gates	*(Instruction to SEW PM. Specify risk level of fence L / M / H)*
5	Intruder detection	*(Instruction to SEW PM. Specify the number, type and location of detectors if required)*
6	CCTV monitoring	*(Instruction to SEW PM. Specify the number, type and location of CCTV cameras if required)*
7	Detector activated flood lighting	*(Instruction to SEW PM. Specify what flood lighting should be switched by what detectors if required)*
8	Loudspeakers (for alarm &/or voice)	*(Instruction to SEW PM. Specify location and type of speakers if required)*

For a specification for each security risk control, refer to South East Water's full Water and Sewerage Facility Security document AM2759.

Instruction to SEW PM: Complete all blank cells in Table 3, providing information obtained from Customer Service Delivery on what work needs to be completed as part of the project. Delete instruction once task complete.

Table 3: Incidental Threats

Security Risk	Risk Level: not present - L / M / H.
Falling limbs / trees	
Bushfire	
Flood	
Storms (wind & lightening)	
Vehicle strike	
Livestock	

Instruction to SEW PM: Remove all unrequired controls (rows) from Table 4 & edit as required in consultation with Customer Service Delivery. Delete instruction once task complete.

Table 4: Incidental Threat Risk Control Options to be Implemented

ID	Risk Control Description	Required Y / N. Specification
1	Plant and equipment contained within locked buildings, cubicles, tanks or chambers.	
1	High bush fire risk area. If Yes, BAL ratings will need to be calculated for each above ground plant location.	
1	*XXXX* items require submersion proof housing.	*(Instruction to SEW PM. Describe what items may be subject to flooding)*
4	Security fencing and locked gates	*(Instruction to SEW PM. Specify risk level of fence L / M / H. Delete if replicated above)*
6	CCTV monitoring	*(Instruction to SEW PM. Specify the number, type and location of CCTV cameras if required. Delete if replicated above)*
10	Facility Location and Set Out of Assets within Facilities	Y. *(Instruction to SEW PM. Specify any known areas of the land in which plant and equipment should not be located)*
11	Vegetation Management	*(Instruction to SEW PM. Specify any vegetation that needs to be removed or trimmed)*
12	Bollards and barriers	
13	Water / sewage storage	*(Instruction to SEW PM. Specify if and what type of emergency storage is required- if not already done so)*
13	Backup power	*(Instruction to SEW PM. Specify if and what type of backup power is required)*
14	Livestock barbed wire outer fencing	*(Instruction to SEW PM. Specify if external land has or likely will have livestock around the perimeter)*

For a specification for each security risk control, refer to South East Water's full Water and Sewerage Facility Security document AM2759.