Network Physical Security – Design Reference

Energy Queensland

Network Physical Security – Design Reference

Revision history

Revision date	Version number	Author	Description of change/revision
1/4/2020	0.1	PT/JL	Draft
6/5/2020	1.0	PT/JL	Endorsed by SASP Mgt team with minor changes

Document approvals

Name	Position title	Signature	Date
Carmelo Noel	General Manager Asset Standards		
Justin Morghem	Manager Corporate Security		

Stakeholders / distribution list

Name	Title	Role
Andrew Meiklejohn	Manager Sub Design & Eng.	User
Nicola Roscoe	GM Grid Projects & Optimisation	User
Shane Meng	Civil & Structural Manager	User

Network Physical Security – Design Reference

CONTENTS

1. INTRODUCTION

1.1. Overview

The outline of this Network Physical Security Design Reference ("This Document") is to provide planners and designers the baseline physical security controls for various asset types within the Energy Queensland Limited (EQL) Network Asset portfolio.

1.2. Purpose

The purpose of This Document is to provide guidance to achieve a consistent approach to applying physical security controls for Network assets and is targeted at EQL internal stakeholders, consultants and architects for the design and application of physical security controls consisting of electronic security systems. This document is not intended to be a detailed design.

This Document does not cover physical security for Non-Network Assets such as corporate offices, depots, distribution centres, training centres, pole yards. Please refer to the Non-Network Physical Security Design Reference for guidance on the physical security controls available for Non-Network assets.

1.3. Scope

The scope of This Document is limited to guidance on the provision of physical security measures for Network Assets including:

- Bulk Supply Substations;
- Zone Substations; and
- Commercial and Industrial Substation
- Standalone telecommunications sites

This Document recognises that in some applications and circumstances logical security treatments (such as those implemented by the Digital Office) will also contribute to security risk reduction, as part of a layered approach.

Generation assets associated with isolated systems will be covered under separate documentation from the Renewables & Distributed Energy Group.

1.4. Asset/Risk Owners

The asset owner is accountable for the asset or group of assets with a responsibility to ensure control measures are implemented appropriately to reduce the risk exposure to an acceptable level.

Key management is one such control and the asset owner will have a Key Management System as outlined in R154 Access Control guidelines. See section 2.4.1.

1.5. Designers

This Document is a guidance document and is intended to be read at a high level only. Details on design and installation requirements associated with the implementation of security control measures may reside in sources flagged in Section 1.10 Reference sources.

It is the responsibility of the designer to complete all relevant site investigations and identify all relevant compliance requirements and approvals (both EQL and external) required to complete the design and construction of security measures referred to in This Document and any specific, relevant project or contract documentation.

1.6. Non-prescription

The physical security treatment measures detailed in This Document are not meant to be prescriptive in nature or requirement. Ultimately, the treatment of the security risks is achieved by applying the

results of a security risk assessment and/or as per the general advice provided in This Document to ensure the ongoing availability, continuity and resilience of all Network Assets.

1.7. Audience

This document is primarily intended for:

- EQL Network planners, designers and project managers;
- EQL Line Management; and
- EQL Operational Telecommunications staff.

Additionally, This Document should also be referred to by the following external stakeholders with respect to the design, implementation and management of security for Network Assets:

- Architects;
- Builders;
- Electrical Engineers:
- Consultants; and
- any other organisation or person responsible for the design of physical security of EQL people or physical assets.

1.8. Enquiries

Any enquiries are to be forwarded to corporatesecurity@energyq.com.au for review and response.

1.9. Reference documents

This document should be read in conjunction with the following EQL reference documents:

Document Name	Description
EQL Physical Security Technical Reference (draft)	The standard for identifying the technical criteria for physical security.
Network Security Risk Assessment Tool and accompanying guide	A spreadsheet tool and reference guide which standardises the approach towards completing security risk assessments for EQL Network Assets.
Corporate Security - CCTV Guideline (R151)	A document which describes the business requirements for CCTV across its asset base.
Corporate Security - View, Review, Download and Reproduce CCTV Guideline (R152)	A document which describes the business requirements regarding the protection of information generated from CCTV systems.
Corporate Security - ID Card Guideline (R153)	A document which describes the business requirements for the management and administration of identification cards.
Corporate Security - Perimeter Security Guideline (draft)	A document which describes the business requirements for perimeter security across its asset base.
Corporate Security - Security in Construction Guideline (draft)	A document which describes the business requirements for physical security for EQL sites which are under construction.
Corporate Security - Security of Materials Guideline (R150)	A document which describes the business requirements for the security of materials across its asset base.
Corporate Security – Access Control Guideline (R154)	A document which describes the business requirements for access control across its asset base.
Australian Government – Physical security management guidelines	Provides guidance on achieving a consistent approach to determining physical security controls

Energex RED 375	Substation Security - Key Tactical and Operational Requirements
Energex StdsA271	Changes to Substation Security Fence Design
LOSTD-CV019 (all sheets)	Energex Substation Security Fencing Drawings
Ergon Drawing No EESS-10078-01 & 02	Substation Standards. Standard Security Fencing. Construction Details.

1.10. Reference sources

The design reference does not diminish the designer's obligation to ensure the design of physical security controls should complies with the following reference documents:

- Queensland Government CPTED Part A & B Guideline
- AS/NZS 2201 Set:2008 (Intruder Alarm Systems)
- AS/NZS 4806:2008-Set (CCTV)
- AS/NZS 1768:2007 (Lightning Protection)
- AS/NZS ISO 31000:2009 (Risk Management – Principles and Guidelines)
- AS 1725.1:2010 (Chain-link fabric security fencing and gates – General Requirements)
- AS 2067:2016 (Substation and high voltage installations exceeding kV a.c)
- AS/NZS 3016:2002 (Electric Security Fence)
- AS/NZS 4421:2011 (Guards and Patrol Security)
- ENA DOC 015-2006: (National Guidelines for Prevention of Unauthorised Access to Electricity Infrastructure)
- HB167:2006 – (Security Risk Management Handbook)
- Information Privacy Act 2009 (Qld)
- Public Records Act 2002 (Qld)
- Security Providers Act 1993 (Qld)
- Queensland Government CCTV Guidelines
- Queensland Government Information Standard 18: Information Security
- Queensland Government Information Security 31: Retention and disposal of public records
- Queensland Government Information Standard 40: Recordkeeping
- Managing CCTV records – Guideline for Queensland Public
- Federal Government, Protective Security Policy Framework – PSPF

1.11. Acronyms and abbreviations

The following acronyms and abbreviations may have been used throughout this document:

Acronym/abbreviation	Full meaning
2FA	Two factor authentication
A/V	Audio visual
AC	Alternating current
AFL	Above floor level
AOB	Any other business

Acronym/abbreviation	Full meaning
BCA	Building code of Australia
CCTV	Closed circuit television system
CoC	Certificate of compliance
D&C	Design and construct
DA	Development approval
DC	Direct current
DOTL	Door open too long
EACS	Electronic access control
ELM	End of line module
ELV	Extra low voltage
EQL	Energy Queensland Limited
FoV	Field of view
GUI	Graphical user interface
HVAC	Heating ventilation and cooling
ICT	Information and communications technology
IDS	Intruder detection system
IPS	Images per second
IT	Information technology
IVA	Intelligent video analytics
KVM	Keyboard video mouse
LAN	Local area network
MVA	Mega Volt Amp
NCC	National construction code
VMS	Video management system
PA	Public address
PE	Photo-electric
PoE	Power over Ethernet
PPM	Pixels per meter
PTZ	Pan-tilt-zoom
QoS	Quality of service
QPS	Queensland Police Service
RTU	Remote terminal unit
SMS	Security management system
SNMP	Simple network monitoring protocol
SRA	Security risk assessment
SVC	Static var compensator
TCA	Telecommunications cabling advice
TCP/IP	Telecommunications control protocol/internet protocol
UPS	Uninterruptable power supply
UTP	Unshielded twisted pair
V	Volts
VBIED	Vehicle borne improvised explosive device
VLAN	Virtual local area network
WBS	Work break-down structure

1.12. Limitations

This document does not contain any site-specific information, nor should it be considered a detailed or complete design.

It is the responsibility of the EQL designer, service provider, engineer or security system designer to complete all required site investigation and design in compliance with the requirements of this document and the contract for which they have been engaged by EQL.

2. APPROACH

2.1. General

Baseline security controls are identified as items or devices used to provide a minimum level of security, typical examples used are:

- Defined perimeter (i.e. fence, gates, doors etc.);
- Nominated entry points (i.e. doors or gates requiring restricted key system or access control for entry);
- Monitoring of entry points (i.e. reed switches on doors, detection devices);
- Surveillance (i.e. natural surveillance by maintaining clear unobstructed fence lines, continual observation by EQL staff and CCTV systems); and
- Securing attractive or valuable items (i.e. locking copper and tools in secured containers).

2.2. Philosophy

This design reference provides guidance on the baseline requirements for the implementation of security measures within EQL owned or operated Network Assets (substations).

This document provides advice on the application of approved security controls relative to the operational areas associated with an asset or sub-asset (See Figure 1):

- Zone 1: The boundary of the Network Asset (e.g. substation perimeter), taking in all assets enclosed within the perimeter.
- Zone 2: Facilities, control buildings, switch rooms, fully enclosed transformer rooms, sheds, generator compounds etc within Zone 1.
- Zone 3: Equipment rooms with exposed HV terminals, and/or rooms within Zone 2 containing sensitive equipment in racks and/or enclosures.

(Note all HV enclosures shall comply with the requirements of AS2067, Electrical Safety Act, Energy Queensland rules and plant and equipment standards).

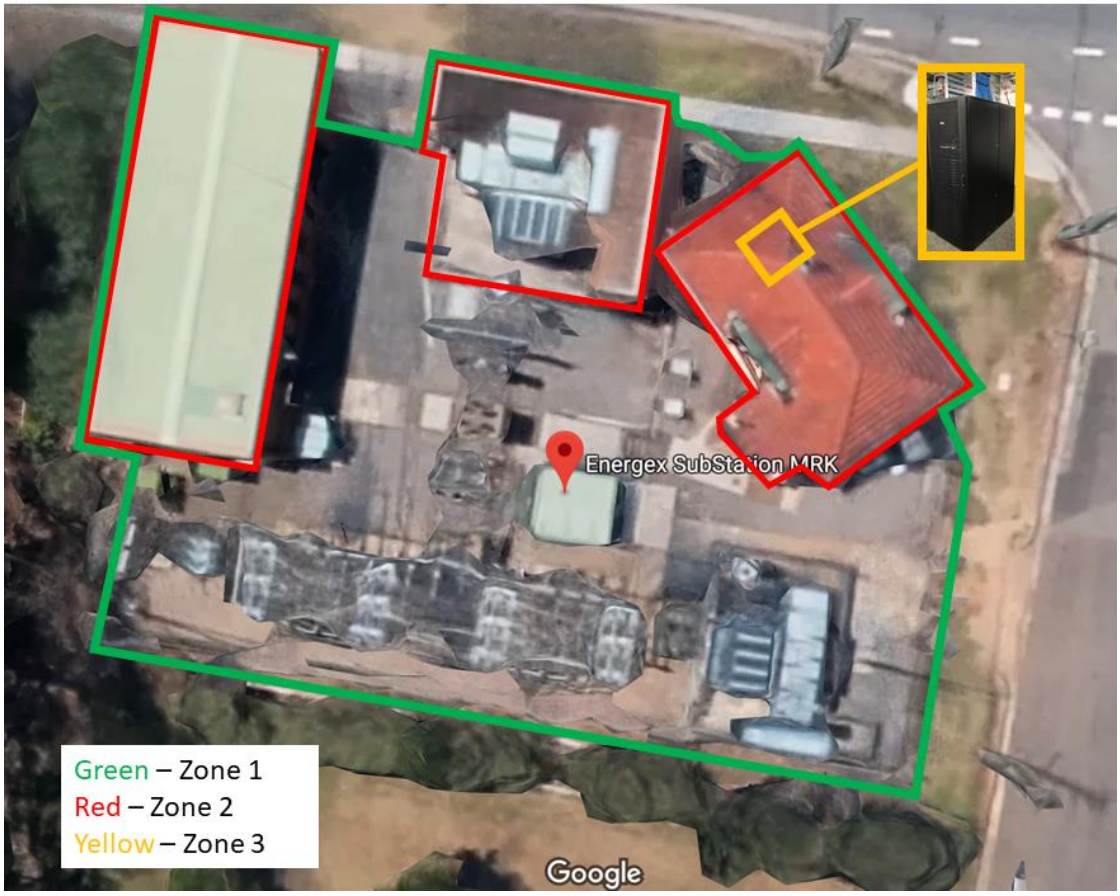

Figure 1 – Definition of Zones in Substation

The level of security assurance is relative to the risk profiling, application of security controls and site management of security procedures. The zone type is the reference term used to identify operational areas, each with a range of recommended security controls. Generally, access to operational areas shall progressively increase through the application of multiple layers of physical and logical security controls, to increase the 'Security-in-Depth' of the Asset.

This Document also recognises that in some cases the application of multiple concentric security measures will not be achievable (for example, at a non EQL controlled site) and asset protection will be limited to standalone measures implemented at the discretion of the Asset/Risk Owner.

2.3. Security Risk Assessment (SRA)

A Security Risk Assessment must be completed prior to the project approval stage so that sufficient funds may be allocated to the project. The level of assessment depends on the classification of the asset (see Section 3.2)

- Critical - Refer to EQL Security Risk Assessment process for further details. To be conducted by Corporate Security team or their representative
- High, Significant or Limited – existing RED 375 using the ENA 015 assessment criteria can be used.

All results shall be recorded in EQL's Substation Security & Vulnerability Register. The relevant manager identified in the risk assessment shall sign off on the level of security risk. Measures identified in Section 5 can be used to reduce the level of risk. See table below for authorisation tables based on RED375 assessment for non-critical sites.

Risk Tolerability Authorisation Table (extract from RED375)			
Vulnerability score	***Risk* Descriptor**	**Risk Tolerability Criteria and Authorisation Requirements**	
≥86	***Very High Risk***	***Risk*** must be managed in line with the **ALARP** Principles	**Executive Management Team Approval** *(required to continue risk exposure)*
85	***High Risk***		**Divisional Manager/ Executive General Manager Approval** *(required to continue risk exposure)*
65	***Medium Risk***		**Group Manager/Process Owner Approval** *(required to continue risk exposure)*
49	***Low Risk***		**Line Manager (or equivalent) Approval** *(required to continue risk exposure)*
≤39	***Very Low Risk***		**Supervisor/Coordinator Approval (or equivalent)** *(required to continue risk exposure)*

2.4. Primary Controls

Primary Controls are used to identify the property boundary and is defined by installation of a fence and access gates. The following documents detail the minimum design criteria for primary controls:

a. ENA DOC 015 – National Guidelines for the Prevention of Unauthorised Access to Electricity Infrastructure; and

b. AS 2067:2016 – Substations and High Voltage Installations Exceeding 1 kV a.c.

Where not specifically directed by the results of a security risk assessment, EQL Network planners and designers shall refer all fence and gate design requirements to the above two standards and the relevant internal fence/gate specifications/drawings. The site risk assessment and/or business specific requirements may trigger additional security controls (referred to in ENA-015 as secondary security controls) as shown below.

This Document may also refer to Primary Controls associated with architectural elements of the Asset yet omits provision of any specific guidance on their implementation. Designers are required to identify and reference relevant EQL documentation with regards to architectural related Primary Controls.

2.4.1 Key Management

Asset Managers are accountable for the asset or group of assets with a responsibility to ensure control measures are implemented appropriately to reduce the risk exposure to an acceptable level.

Key management is one such control and the asset owner's delegated representative will have a Key Management System as outlined in R154 Access Control guidelines.

2.5. Secondary Controls

Secondary Controls consist of additional security hardware to assist in providing the management of authorised access or to add another layer of security to the primary control. ENA Doc-015 outlines typical secondary controls that can be implemented in substations. EQL Corporate Security can provide additional design input and advice for secondary controls where there may be site specific influences that do not fit within the standard substation design. Examples of secondary security controls may consist of:

a. Access Control Systems;

b. Intrusion Detection Systems;

c. Closed Circuit Television (CCTV);

d. Electric Fence/Fence Detection Systems;

e. Intercom System and Public Address (PA) systems; and

f. Perimeter Intruder Detection Systems.

2.6. Communications and cabling

Security cameras, IP PA speakers and other networked secondary controls shall be installed on their own VLAN. In general, they will have their own network switch, although in cases where there are only one or two devices and there is room on the existing network switches these may be used, provided at least one port remains available on each switch for OTN use, Security systems in secondary buildings to have a separate subnet as well. Further advice can be obtained from Telecommunications Department.

Preference is for cabling from the VLAN to secondary control devices to be fibre optic. If copper cable is used (Ethernet, RS485) it shall be screened or run in a separate conduit to power cables to avoid problems with electrical induction.

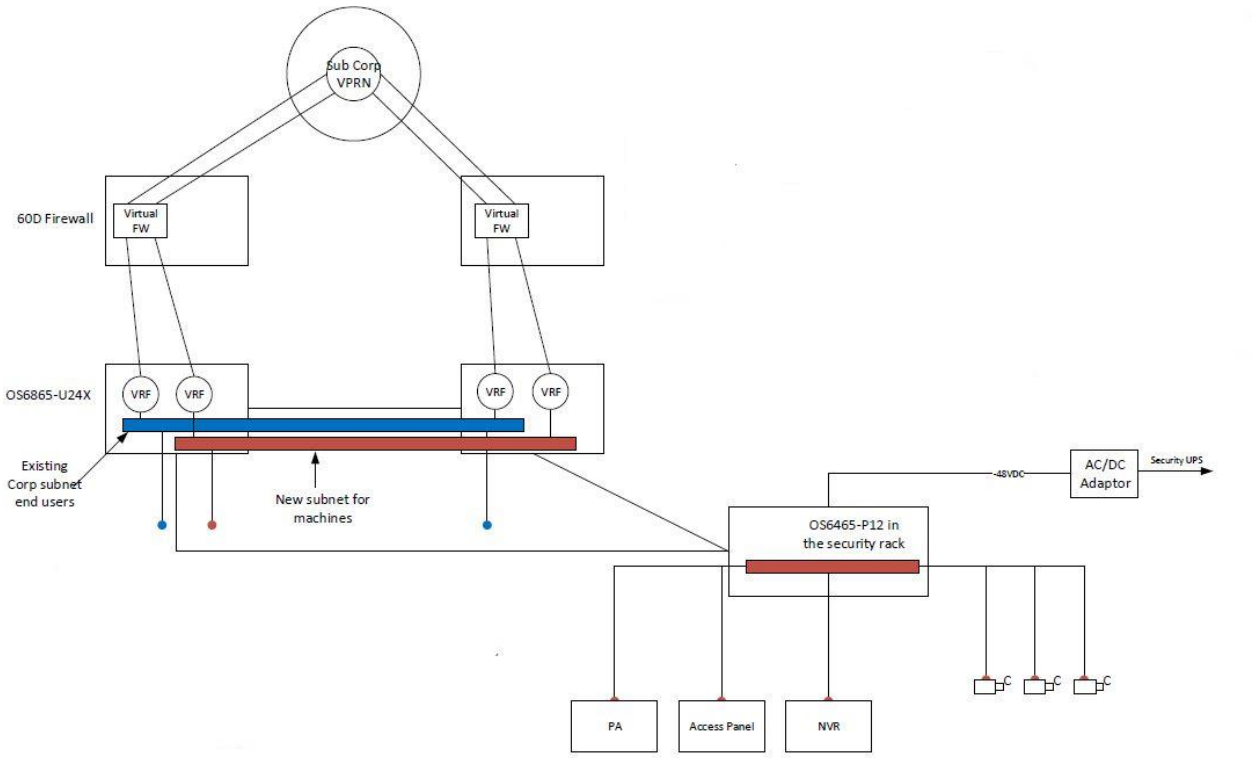

Figure 2- Typical Telecommunications configuration.

3. SECURITY DESIGN STANDARDS

The underlying principle in applying baseline physical security controls is to limit unauthorised access while being able to accurately identify and record details relating to authorised personnel access to Network assets.

This section provides a high-level view of 'Security-in-Depth' principles and how the asset classification, asset types and different work areas within these locations are required to have a diverse range of security controls.

3.1. Security-in-depth

EQL applies a 'Security-in-Depth' approach towards physical security controls to reduce the likelihood and severity of attacks from malicious actors and to ensure high-voltage enclosures are not readily accessible by unauthorised persons. A more resilient security environment is achieved by the layering of different types of physical security controls which will together provide greater protection of EQL people, assets and information.

Security controls when applied in a 'Security-In-Depth' approach shall be designed to Deter, Detect, Delay, Deny and Respond to a source of security threat.

The relationship between detecting the breach and the response process is illustrated in Figure 3:

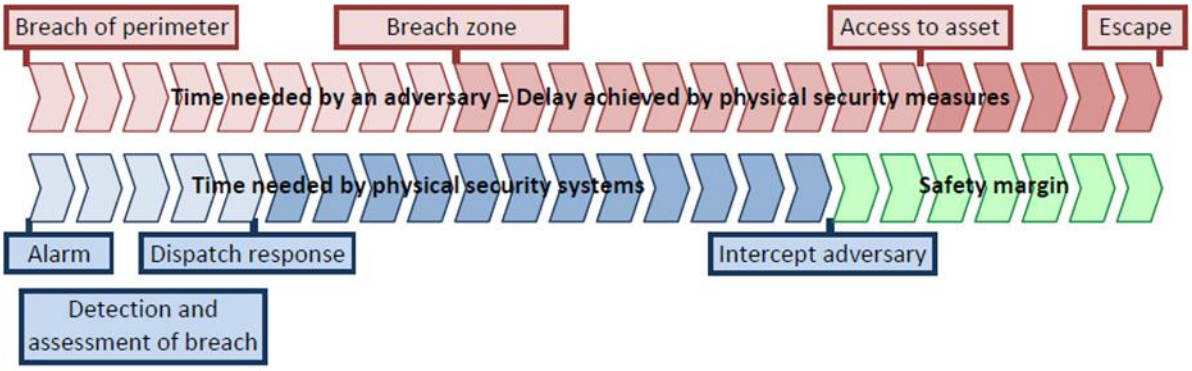

Figure 3- Breach and response

3.2. Asset classification and security controls

An EQL Network Asset can be classified as either:

- Critical;
- High;
- Significant; or
- Limited.

The classification of an EQL Network Asset is based on the level of importance it has to the business. The criterion used to determine Asset Classification has been developed by EQLs Corporate Risk Group and considers several factors influencing the organisations risk exposure in the event a Network Asset is lost, compromised or functionally degraded.

EQL Network Asset/Risk owners should refer to the following guidance published by the Corporate Risk Group when determining the classification of a Network Asset:

- EQL Standard S021 – Standard for Risk Management
- EQL Reference R056 – Risk Evaluation (Consequence & Likelihood) Matrix

The classification of the asset will carry implications for both the context and protective security measures required for its protection. Additionally, certain assets may require a balanced approach as the asset may reside within certain locations/buildings/sites which do not fall into any specific category. In this case, EQL Corporate Security can provide guidance to the business and assess the security to determine the most appropriate security controls.

As a guide, the following table may offer criteria for evaluation of the asset classification:

Asset Classification	Asset Type	Impact to Community
Critical	Installed transformer capacity ≥100MVA SVC: provides network stability for load and major embedded generation Connection asset market participant ≥100MVA Telecommunications sites containing centralised Telecommunication network management systems • Key strategic node sites containing MPLS, Microwave and TDM (SDH / PDH) networks	≥ 20,000 customers or significant CBD loads Load at risk > 50MVA Major industrial customers whose production is critically affected by even short time outages (refineries, smelters) Severe community outrage at loss of service Outage would cause severe impact on CBD reliability/STPIS
High	Installed transformer capacity 50 – 99 MVA Connection asset market participant between 30 and 100MVA Telecommunications sites containing: • One or more MPLS nodes • Multiple DB2 / DB4 or DM2 PDH multiplex equipment • Single DN2 node	Between 10,000 to 20,000 customers Load at risk 25-50 MVA Major customers whose may have backup generation but may be affected by long time outages (hospitals, shopping centres) Community outrage if extended loss of service Outage would cause severe impact on urban reliability/STPIS
Significant	Installed transformer capacity 20 - 49 MVA Telecommunications sites containing: • MPLS long line switch / CE node • Single DB2 / DB4 or DM2 PDH node	2,500 to 10,000 customers Load at risk 10-25 MVA Community upset at loss of service Outage would cause moderate impact on urban or severe impact on rural reliability/STPIS
Limited	Installed transformer capacity <20 MVA Telecommunications sites containing simple modem	Less than 2 500 customers Load at risk < 10 MVA Community disquiet at loss of service Outage would cause moderate impact on rural reliability/STPIS

Where one criteria may be higher than another the higher classification shall be taken for the asset.

4. SECURITY ZONES

Following the classification of a Network Asset by the Asset/Risk owner, the Asset/Risk owner must assess the requirement for completion of a security risk assessment, including application of protective security zones to achieve an appropriate level of 'Security-in-Depth' for the site.

The table below outlines security zones typically associated with an Asset, based on their classification. It also provides guidance on when the security risk assessment process should be adopted, based on Asset classification (refer Figure 1 for definition of zones):

Asset Classification	Zone 1	Zone 2	Zone 3	SRA
Critical	✓	✓	✓	Mandatory
High	✓	✓	✓	Highly recommended
Significant	✓	✓		Recommended
Limited	✓			Discretionary

4.1. Treatment guidance matrix

The matrix below establishes a series of baseline security treatments approved by EQL Corporate Security, at the disposal of an EQL Asset/Risk owner to reduce inherent security risk exposure.

To assist EQL Asset/Risk owners, EQL Corporate Security has assigned treatment measures to each discrete zone/classification type, to ensure a baseline level of protection is achieved.

The EQL Asset/Risk owner is responsible for the selection and implementation of treatment measures, based on site limitations and constraints influencing inherent risk levels and the specific assets' operating environment.

TREATMENT/MEASURE	CRITICAL			HIGH			SIGNIFICANT			LIMITED		
	Z1	Z2	Z3	Z1	Z2	Z3	Z1	Z2	Z3	Z1	Z2	Z3
Chain-link perimeter fence to AS 2067 & AS 1725				●			●			●		
Palisade perimeter fence to ENA-015	●											
Weldmesh perimeter fence to ENA-015	●			●								
Gates to same standard as perimeter fence	●			●			●			●		
Commercial grade locking systems	●	●		●	●		●	●		●	●	
Protected padlock and chain	●			●			●			●		
Window grilles and locks		●			●			●		●		
External LED lighting with auto sensor PE	●			●								
Perimeter video surveillance, (PTZ)	●			●								
Asset video surveillance			●									
General video surveillance	●	●		●	●		●	●				
Electronic access control, entry reader	●	●		●	●		●	●		●		
Intruder alarm system coverage (perimeter)	●	●		●	●			●			●	
Intruder alarm system coverage (internal)		●			●			●			●	
TREATMENT/MEASURE	Z1	Z2	Z3	Z1	Z2	Z3	Z1	Z2	Z3	Z1	Z2	Z3
Perimeter Intrusion Detection				●								
Electric Fencing System	●											
IP PA speaker for VoIP announcements	●			●			●					

Security signage	●	●		●	●		●	●		●		
Arm/disarm indicator	●	●		●	●		●	●		●		

5. IMPLEMENTATION GUIDANCE

5.1. Security of 'Critical' assets

The table below provides guidance on the selection and implementation of physical security control measures associated with security zones for assets classified as 'Critical':

No.	Function	Guiding Principles
1	Zone 1 – Generally operational areas within the perimeter fence/yard area containing outdoor HV plant and Zone 2 enclosures. Includes substation earth grid and connections, and any equipment stored permanently or temporarily at site.	Unless directed otherwise by the results of a security risk assessment, Zone 1 areas for 'Critical' Assets should be implemented as follows: • Weldmesh or palisade perimeter fencing to ENA-015, inclusive of anti-climb and anti-tunnel measures • Full height pedestrian gates to control primary pedestrian entry/egress • Electric fence for the full perimeter of the site (Note – shared fences may need to be solid to prevent landscaping from neighbours interfering with electric fence operation) • Primary perimeter entry/exit points to be monitored and controlled by the intruder detection and access control system, entry reader • All other perimeter gates are to have a protected padlock and chain based on EQL restricted keying system • Fixed CCTV cameras to view nominated access path from perimeter gate to entry doors of buildings • Fixed CCTV cameras to provide general coverage of typical movement areas around buildings • PTZ cameras located on buildings to provide as much coverage of the perimeter electric fence (maximum 2 x PTZ cameras) • Low level LED lighting operated by PE cell to support CCTV and natural surveillance • Arm/Disarm indicators as indicated by the specification or shown on standard drawings • External environmental enclosure to accommodate security equipment if the security equipment is not located inside the control buildings • IP PA speaker for voice announcements • Security and electric fence signage • All transformers are enclosed, or if outdoors have HV and LV cable boxes ***where practical***. Consideration given to indoor GIS and cable entry to eliminate exposed busbars ***where cost justifiable***.
2	Zone 2 – Facilities, control buildings, switch rooms, enclosed transformer compounds, sheds, generator compounds etc.	Unless directed otherwise by the results of a security risk assessment, Zone 2 areas for 'Critical' Assets should be implemented as follows: • All primary entry/exit perimeter doors to be provided with access control monitored and controlled by the EQL corporate intruder detection and access control system, entry reader • All other doors/openings to be provided with door monitoring device connected to the alarm system

No.	Function	Guiding Principles
		• Motion detectors to be provided to rooms with external windows or doors on ground floor; and higher floors if accessible from external of the building • Registered lock and key cylinders • Security signage • Arm/Disarm indicators as indicated by the specification or shown on standard drawings • All MV and GIS switchgear installed with Zone 2 secured building.
3	Zone 3 – Equipment rooms,	No specific additional security measures, unless specifically identified as part of a site risk assessment. If required additional measures could include: • CCTV oversight of the target asset •

5.2. Security of 'High' assets

The table below provides guidance on the selection and implementation of physical security control measures associated with security zones for assets classified as 'High':

No.	Function	Guiding Principles
1	Zone 1 – Generally operational areas within the perimeter fence/yard area containing outdoor HV plant and Zone 2 enclosures. Includes substation earth grid and connections, and any equipment stored permanently or temporarily at site.	Unless directed otherwise by the results of a security risk assessment, Zone 1 areas for 'High' Assets should be implemented as follows: • Weldmesh or chain-link perimeter fencing to ENA-015, inclusive of anti-climb and anti-tunnel measures • Full height pedestrian gates to control primary pedestrian entry/egress • Perimeter intrusion detection for the full perimeter of the site • Primary perimeter entry/exit points to be monitored and controlled by the intruder detection and access control system, entry reader • All other perimeter gates are to have a protected padlock and chain based on EQL restricted keying system • Fixed CCTV cameras to view nominated access path from perimeter gate to entry doors of buildings • Fixed CCTV cameras to provide general coverage of typical movement areas around buildings • PTZ cameras located on buildings to provide as much coverage of the perimeter electric fence (maximum 2 x PTZ cameras) • Low level LED lighting operated by PE cell to support CCTV and natural surveillance • Arm/Disarm indicators as indicated by the specification or shown on standard drawings • External environmental enclosure to accommodate security equipment if the security equipment is not located inside the control buildings • IP PA speaker for voice announcements • Security signage

No.	Function	Guiding Principles
2	Zone 2 – Facilities, control buildings, switch rooms, enclosed transformer compounds, sheds, generator compounds etc.	Unless directed otherwise by the results of a security risk assessment, Zone 2 areas for 'High' Assets should be implemented as follows: • All primary entry/exit perimeter doors to be provided with access control monitored and controlled by the EQL corporate intruder detection and access control system, entry reader • All other doors/openings to be provided with door monitoring device connected to the alarm system • Motion detectors to be provided to rooms with external windows or doors on ground floor; and higher floors if accessible from external of the building • Registered lock and key cylinders • Security signage • Arm/Disarm indicators as indicated by the specification or shown on standard drawings • Where cost justifiable and practical, MV switchgear installed with Zone 2 secured building.
3	Zone 3 – Equipment rooms	No specific additional security measures, unless specifically identified as part of a site risk assessment. If required additional measures could include: • CCTV oversight of the target asset

5.3. Security of 'Significant' assets

The table below provides guidance on the selection and implementation of physical security control measures associated with security zones for assets classified as 'Significant':

No.	Function	Guiding Principles
1	Zone 1 – Generally operational areas within the perimeter fence/yard area containing outdoor HV plant and Zone 2 enclosures. Includes substation earth grid and connections, and any equipment stored permanently or temporarily at site.	Unless directed otherwise by the results of a security risk assessment, Zone 1 areas for 'Significant' Assets should be implemented as follows: • Chain-link perimeter fencing to ENA-015, inclusive of anti-climb and anti-tunnel measures • Full height pedestrian gates to control primary pedestrian entry/egress • Primary perimeter entry/exit points to be monitored and controlled by the intruder detection and access control system, entry reader • All other perimeter gates are to have a protected padlock and chain based on EQL restricted keying system • Fixed CCTV cameras to view nominated access path from perimeter gate to entry doors of buildings • Fixed CCTV cameras to provide general coverage of typical movement areas around buildings • Low level LED lighting operated by PE cell to support CCTV and natural surveillance • Arm/Disarm indicators as indicated by the specification or shown on standard drawings

No.	Function	Guiding Principles
		• External environmental enclosure to accommodate security equipment if the security equipment is not located inside the control buildings • IP PA speaker for voice announcements • Security signage
2	Zone 2 – Facilities, control buildings, switch rooms, enclosed transformer compounds, sheds, generator compounds etc.	Unless directed otherwise by the results of a security risk assessment, Zone 2 areas for 'Significant' Assets should be implemented as follows: • 1 xl primary entry/exit perimeter doors to be provided with access control monitored and controlled by the EQL corporate intruder detection and access control system, entry reader • All other doors/openings to be provided with door monitoring device connected to the alarm system • Motion detectors to be provided to rooms with external windows or doors on ground floor; and higher floors if accessible from external of the building • Registered lock and key cylinders • Security signage • Arm/Disarm indicators as indicated by the specification or shown on standard drawings
3	Zone 3 – Equipment rooms,	No specific additional security measures, unless specifically identified as part of a site risk assessment

5.4. Security of 'Limited' assets

This Asset class will typically only require a single security zone, based on the profile and location of their operating environment. Unless specifically directed by the results of a security risk assessment, Assets of this classification will generally omit the provision of electronic security measures in favour of more robust physical security measures designed to delay or deny access to the Asset.

Stand-alone assets may require more simplistic controls such as pad-locks and signage; while assets in third party rooms/building may be able to have access control, CCTV and intrusion detection devices.

The table below provides guidance on the selection and implementation of physical security control measures associated with security zones for assets classified as 'Limited':

No.	Function	Guiding Principles
1	Zone 1 – Generally operational areas within the perimeter fence/yard area containing outdoor HV plant and Zone 2 enclosures. Includes substation earth grid and connections, and	Unless directed otherwise by the results of a security risk assessment, Zone 1 areas for 'Limited' Assets should be implemented as follows: • Chain-link perimeter fence/cage/barrier to AS 2067 & AS 1725 including anti-climb and anti-tunnel, where appropriate • Access portals (gates, cage doors etc) to the same standard as the perimeter fence/cage/barrier • For stand-alone assets, all access panels and perimeter gate entrance to have a protected padlock and chain based on EQL restricted keying system

No.	Function	Guiding Principles
	any equipment stored permanently or temporarily at site.	• 1 x primary entry/exit perimeter doors to be provided with access control monitored and controlled by the EQL corporate intruder detection and access control system, entry reader • All other doors/openings to be provided with door monitoring device connected to the alarm system • Security signage