January 2026

Powerlink 2027-32 Revenue Proposal

Protective Security Strategy

Powerlink Protective Security – Strategy

Management System	Asset Management	
Authored by	Manager Protective Security & Authorisations	[redacted]
Reviewed by	General Manager Operational Engineering	[redacted]
Approved by	Chief Operating Officer	[redacted]

Version History

Version	Date	Section(s)	Summary of amendment
1.0	26/05/2025		Original

Table of Contents

PROTECTIVE SECURITY STATEMENT

Powerlink's Commitment to Protective Security

Powerlink is steadfast in its commitment to ensuring the protection of its people, information, and assets from acts of unlawful interference and other significant security threats. We recognise the importance of safeguarding our critical infrastructure and minimising security risks to a level that is as low as reasonably practicable.

As owners and operators of vital critical infrastructure, our foremost priority is to ensure the safety of our people and assets while maintaining the uninterrupted delivery of services.

To achieve this, we must:

- Ensure people and assets are adequately secure from unauthorised access and/or harm
- Be individually accountable and incorporate security risk management in aspects of our planning and work.
- Understand our security threats and vulnerabilities and prepare plans to deal with these threats if they arise.
- Engage the Powerlink's Protective Security Team on standards and advice at the initiation stage of any project or business change activity which has a physical security impact to our people and/or assets.
- Maintain and continuously improve our security risk management framework.
- Minimise the consequences of security threats by developing appropriate business response and recovery plans - and testing these as appropriate.
- Accurately report security incidents at the earliest possible opportunity.
- Apply sound, efficient and economically responsible treatments to reduce the likelihood and consequences of security risks.
- Review the effectiveness of our protective security risk management against relevant metrics.
- Ensure the confidentiality, integrity and availability of Powerlink' information assets and ICT systemsComply with relevant legislation.

Collective Responsibility:

The security of Powerlink's operations is a shared responsibility. Every employee, contractor, visitor, and business partner must proactively contribute to the safeguarding of our organization's people, assets, and information.

Powerlink acknowledges the dynamic and evolving nature of the security threat environment faced by critical infrastructure operators. By fostering a culture of security awareness and responsibility across all levels of the organisation, we will continue to protect our people, assets, and information from harm.

[redacted]

Chief Operating Officer

May 2025

Commitment to Protective Security

SECURITY IS EVERYONE'S RESPONSIBILITY

With the creation of the new Protective Security Team, it is important to emphasise the critical importance of a comprehensive and proactive security strategy in safeguarding our people, assets, data, reputation and keeping our network free from interruption. In today's rapidly evolving security landscape, threats are becoming increasingly sophisticated and diverse, from cyber-attacks to physical security breaches. It is imperative that we stay ahead of these risks through a layered approach to security, combining cutting-edge technology, rigorous protocols, and a culture of vigilance and awareness across all levels of the organisation.

Our security strategy must not only focus on preventing incidents but also on ensuring quick and effective responses to any breaches that may occur. This includes developing strong incident response plans, informative training for our staff, and fostering partnerships with law enforcement and industry experts. Security is not just an IT or physical infrastructure issue but an organisational mindset that impacts every department and function.

By prioritising security in our planning, we protect not only our tangible assets but also the trust and confidence our community, partners, and stakeholders place in us. A robust security framework protects our people, ensures continuity of service, supports compliance with regulatory requirements, and mitigates the potential for financial, legal, and reputational harm.

As we move forward, we must remain agile, continually assessing emerging threats and refining our strategy to adapt to the evolving landscape. Security is not a one-time effort but an ongoing commitment, and it is through this commitment that we will continue to safeguard our organisation's future and long-term success.

Security is a shared responsibility. We ask for your support in keeping a consolidated focus on protecting our people, facilities, systems and network. By working together, we can continue to ensure a safe and secure environment for everyone. The strength of our security framework relies not only on the systems and processes in place but also on the vigilance and cooperation of every individual involved.

Your trust is paramount, and we are committed to upholding it by maintaining the highest standards of security and service, ensuring that we remain prepared for any challenges that may arise.

[redacted]

General Manager

Operational Engineering

[redacted]

Manager, Protective Security & Authorisations

Operational Engineering

1. Introduction

1.1 Purpose

It is widely understood that the Nation's critical energy infrastructure faces new threats, challenges and opportunities as the industry evolves. Powerlink as an owner and operator of Queensland's critical infrastructure and essential services provider is responsible for protecting our assets to deliver energy efficiently, safely, reliably and securely to industry sectors.

The dynamic threat environment ensures it is not possible to protect everything at all times so our approach must align with priorities; our responses must be proportionate; as such the costs to deliver an outcome must ensure prudent application and deliver risk reduction outcomes.

The Protective Security team have enterprise-wide responsibility for Protective Security and must ensure capability, systems and processes are in place that are scalable, flexible and adaptable to accommodate a diverse asset base and to deliver a whole of business capability while assessing internal and external (both current and emerging) issues.

Protective Security is a key element of organisational resilience, and our fundamental objective is to strengthen security of our people, assets, information systems and facilities.

Our Protective Security Strategy for 2025-2030 focuses on staying ahead of evolving threats and adapting to a rapidly changing environment. We will prioritise the identification of emerging risks through proactive intelligence, continuous monitoring, and the integration of new technologies.

By fostering resilience, embracing innovation, and maintaining a forward-thinking approach, we will ensure the protection of both our assets and our people. In the face of dynamic geopolitical, economic, and technological challenges, we are committed to anticipating future risks and securing a stable, sustainable future for the organisation.

Our strategy sets out the vision, principles and priorities to align appropriate and consistent controls throughout the business with a statewide approach to reduce the residual risk for personnel, customers and other critical infrastructure sectors to an acceptable level in a cost-effective manner.

The success of the Enterprise Protective Security Strategy 2025 – 2030 relies on a whole of business approach, a shared responsibility and unity of purpose.

The Protective Security Team is accountable for business wide physical security service compliance and protection functions, protecting Powerlink from activism, terrorism and criminal activity whilst managing the strategic development and application of enterprise physical security plans, systems and standards to protect our people, assets and operations.

Protective Security Core Belief

Protective Security is a business enabler keeping our people and assets safe and secure.

Protective Security Fundamental Objective

To partner with the business to anticipate, prepare and respond to adverse events, minimising frequency and severity.

1.2 Scope

This strategy incorporates emerging trends in industry and regulatory environments and supports the Corporate Values, Risk Appetite Statements in support of the Powerlink business plan and encompasses the security of physical assets and infrastructure, employees and contractors.

This strategy applies to all Powerlink occupied and/or owned physical assets, property portfolio and Powerlink employees which will, by default, support the protection of co-located assets on our infrastructure owned by our subsidiaries and confirms all Powerlink personnel are responsible for enabling its success.

1.3 References

Document code	Document title
AS/NZS ISO 31000:2009	Risk Management Principles & Guidelines
HB167:2006	Security Risk Management Handbook
AS/NZS 4806:2008-Set	Closed Circuit Television
AS/NZS 4421:2011	Guards and Patrol Security
ASIO T4 Protective Security	Protecting Critical Infrastructure, Selecting Security Systems & Hardware
Rules (LIN23/006)	Security of Critical Infrastructure Act 2018 (the SOCI Act)
ENA DOC 015-2022	National Guidelines for Prevention of Unauthorised Access to Electricity Infrastructure
Private Security Legislation	*Security Providers Act 1993 (Qld)*
CPTED	Queensland Government CPTED Part A & B Guideline
A4678698	Powerlink's Risk Appetite Statements
Our Strategy	Powerlink Business Strategy
AESCSF (SP-2)	Australian Energy Sector Cyber Security Framework – Security Profile 2
PSPF Release 2024	Protective Security Policy Framework – 2024
ENA DOC 015-2022	National Guidelines for Prevention of Unauthorised Access to Electricity Infrastructure

1.4 Defined Terms

Terms	Definition
Protective Security	The function, principles and processes guiding responsibility and accountability for the physical security (and supporting safety outcomes resulting from a physical security event) of Powerlink personnel, assets and information to support the risk measures to deter, detect, delay, respond and recover from protective security related matters. Protective security manages physical security arrangements to enable Powerlink to achieve its critical business objectives
Security of Critical Infrastructure (SoCI)	Security of Critical Infrastructure Act 2018
Critical component	A site, or area within the business that contains critical components that are essential to ensure the proper function of the critical asset (Transmission Network services to the NEM)
Protective Security Policy Framework (PSPF)	The PSPF sets out Australian Government policy across six security domains and prescribes what Australian Government entities must do to protect their people, information and resources, both domestically and internationally.
Energy Networks Australia	Energy Networks Australia (ENA) is the national industry body representing the operators of energy networks in Australia. ENA advocates for policies and regulations that support the development, operation, and sustainability of network service providers, ensuring that they can meet the energy needs of Australians both now and in the future.

Terms	Definition
Government Owned Corporation (GOC)	The Queensland Government established these businesses – Powerlink is a GOC and is bound by a regulatory framework that includes the *Queensland Government Owned Corporations Act 1993*

1.5 Roles and Responsibilities

Who	What
Security is everyone's responsibility	
Powerlink employees, delivery partners and contractors	Are responsible for safeguarding company assets, information, and systems by following all policies, procedures, and protocols established by the organisation. This includes maintaining the confidentiality of sensitive information, reporting any security incidents or potential vulnerabilities and ensuring the physical security of devices and workspaces. All personnel must remain security aware and ensure that all actions and communications align with Powerlink's overall focus on a safe and secure work environment.
Powerlink Team Leaders and Managers	Are responsible for educating their teams about the importance of security, addressing potential vulnerabilities, and ensuring that security concerns are proactively addressed. Leaders should foster a security-conscious culture.
Manager, Protective Security & Authorisations	• Establish security performance measures to monitor procedures to achieve required protections, address risks, counter unacceptable physical security risks, and improve security maturity. • Embed efficient and effective security management awareness and practices by setting the strategic direction for protective security planning and risk management. • Maintain an accurate and current physical security plan to managing the Powerlink's physical security risks and drive improvements to address areas of vulnerability or low compliance • Direct research, analysis and interpretation of complex security threat environment, to prepare high quality and articulate assessment advice on known threats and enhance the decision-making process to mitigate Protective Security vulnerabilities and risks. • Responsible for maintaining and updating the document • Responsible for implementing this strategy within the business
General Manager, Operational Engineering	• Assess organisational physical security risk and formulate security strategy that promotes organisational effectiveness, reduces risks and limits exposure to liability in all areas of physical risk. • Collaborate with Executive Team and provide expert advice to Senior Executives on material physical security risk(s) and manage capability to assess risks, vulnerabilities and complex threats to operations. • Responsible for implementing this strategy within the business

Who	What
Security is everyone's responsibility	
Chief Operating Officer	• Define the strategic direction of Protective Security resources to deliver the physical security plan objectives, strengthen operations and improve the Powerlink's security posture in order to make sound decisions about protective security planning. • Approve sufficient funding within delegation limits, resources and capability to implement security requirements and ensure the security of assets to protect the people, ensuring uninterrupted services to the community • Foster a positive security culture where all personnel understand their responsibilities to manage security risk. • Responsible for approving this document

1.6 Monitoring and Compliance

- This strategy will be reviewed at least every three years.
- Activities will form part of our SoCI reporting and security maturity assessments.

1.7 Risk Management

The strategy serves as a framework that integrates Protective Security management with broader organisational risk management processes. It ensures that physical security risks are systematically identified, assessed, and mitigated in a manner that supports the company's overall risk posture.

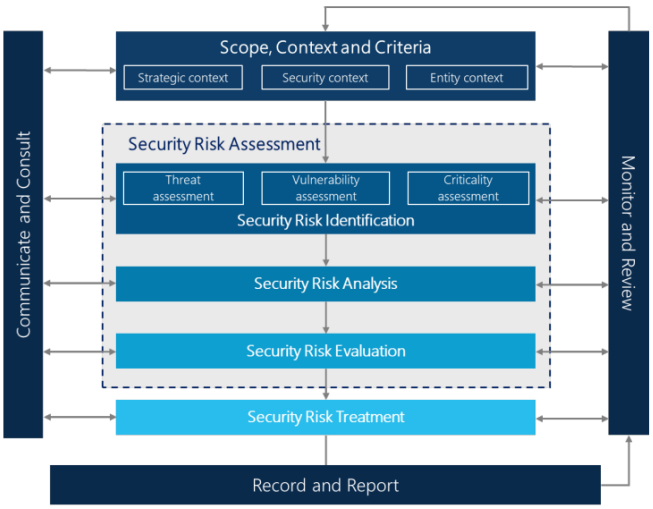


Image 1: Security Risk Management Process

To understand which capabilities to focus on, the Protective Security team need to effectively identify the threats and appreciate the vulnerabilities. Establishing and maintaining strong principles improves our protection against the threats. Understanding the motivation behind the threats greatly supports the business in being able to successfully detect, deter, delay and respond accordingly to achieve the desired outcomes.

Protective Security adopts the Powerlink Risk management approach, including the 7x7 risk assessment matrix that considers the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse impacts that affect Powerlink's ability to meet its objectives.

Image 2: Security landscape risks

1.7.1 Security Risk Analysis

Our approach to risk analysis involves assessing the likelihood and potential consequence of each identified risk, determining the level of risk rating and assessing whether additional controls are required.

With the intent to:

- **Determine control effectiveness** – whether the existing control measures are adequate or effective in managing identified risks.
- **Define the likelihood and consequence** of the event. This is achieved by considering the:
    - Likelihood – the chance or probability of the event occurring, or the probability or frequency of the event (an occurrence or change in a particular set of circumstances, it can be one or more occurrences and can have several causes) occurring.
    - Consequence – the outcome affecting objectives if the event occurs (consequences can be expressed qualitatively or quantitatively and can be certain or uncertain, and have positive or negative effects on objectives). There may be a number of possible outcomes associated with an event.
- **Assign the level of risk rating** based on the likelihood and consequence risk matrix. The overall risk rating is determined by combining the likelihood and consequence estimations. Risk rating allows the security risk to be prioritised in order of decreasing risk levels. This helps with deciding the tolerability of risk in the evaluation step.
- **Prioritise risks** for subsequent evaluation of tolerance or the need for further treatment.
- **Provide an improved understanding of the vulnerability** of critical assets to identified risks.

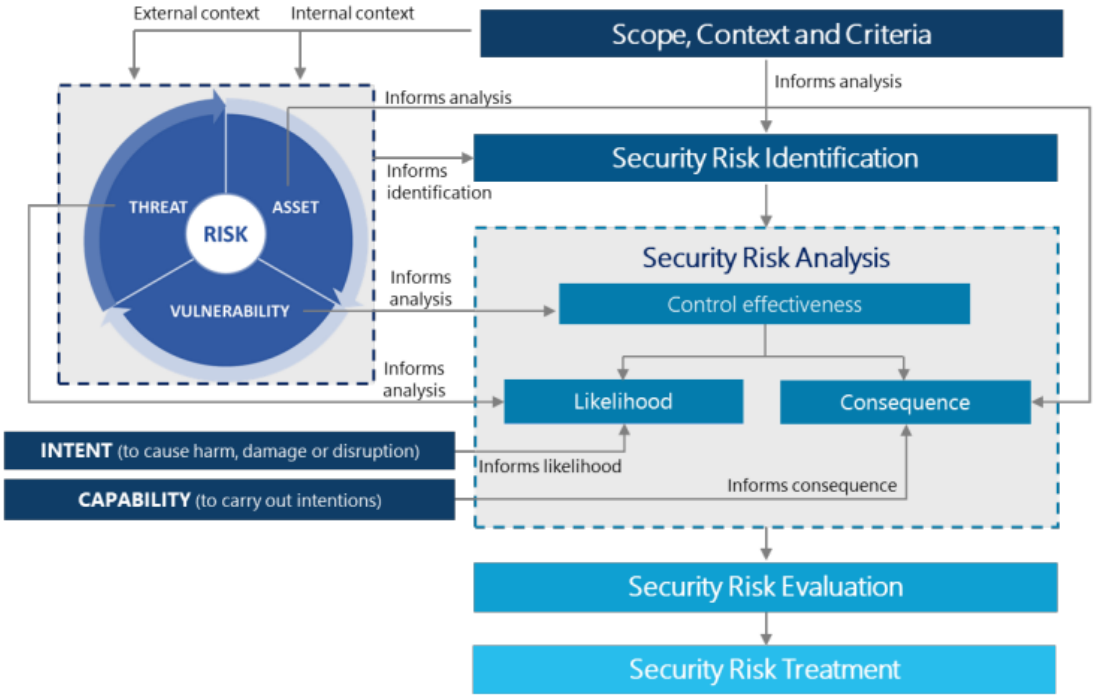
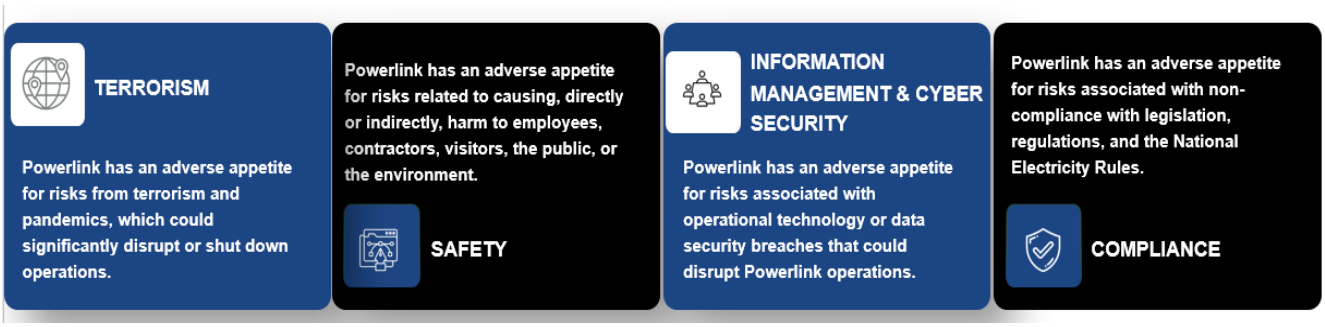


Image 3: Using Threat, Criticality and Vulnerability to Inform Risk Analysis

1.7.2 Risk Appetite Statement Alignment

The strategy security initiatives align with our corporate risk appetite by focusing on the following key areas:

- **Real-Time Monitoring & Emergency Response:**
  The proposal ensures proactive hazard identification and rapid response capabilities, minimizing potential harm and safeguarding employee safety. This aligns with our commitment to reducing risks and ensuring operational continuity in line with acceptable risk levels.
- **Enhanced Protection Against Physical Access Breaches:**
  Strengthening defences against physical security breaches addresses cybersecurity risks, supporting infrastructure protection, and preserving data integrity. This directly supports our stance on minimising cyber risks and maintaining secure operations within tolerable risk boundaries.
- **Compliance & WHS Act Obligations:**
  By reinforcing physical security measures, the proposal ensures compliance with Workplace Health and Safety compliance against relevant regulations, helping us manage risks associated with psychosocial hazards. This supports our objective in maintaining a safe workplace, our regulatory compliance and avoiding penalties or reputational damage, in line with our risk tolerance for legal and compliance risks.



2. Background

2.1 Context

Powerlink faces a challenging threat environment, not in isolation, but in lockstep with industry partners and government.

As such, Powerlink will work toward a multi-layered approach by setting our expectations of a strong security culture in our Physical Security approach and adopting best practices through leading in security technology and government-endorsed and mandated frameworks.

This reinforces the principles of defence-in-depth, an all-hazards approach for risk management, and continuing to leverage relationships with law enforcement and intelligence agencies to ensure we take a comprehensive approach to physical security.

As a statewide supplier, critical infrastructure provider and GOC we face an evolving, complex and dynamic threat landscape as we remain an essential service provider with significant downstream dependencies to the Queenslanders and the wider NEM.

We recognise that the scale and importance of the transmission network makes us a target for a myriad of threats across all security areas - both domestic and international. That is why it is critically important that we know and understand the threat landscape using the context of an all-hazards security model with a comprehensive appreciation of our vast attack surfaces. Our future security capability and organisational resilience will be directly impacted by these ongoing developments, but we will remain ready.

2.1.1 Our Protective Security Approach at Powerlink

Powerlink's approach to Protective Security is a hybrid model - incorporating key elements of the Protective Security Policy Framework (PSPF) and the Energy Networks Australia - Protection of Electrical Infrastructure guidance.

In addition, Powerlink must comply with the Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules which mandates compliance with the AESCSF (Australian Essential Security Controls for the Security framework).

Powerlink has adopted these frameworks to ensure a comprehensive and robust approach to protective security, aligning with national and industry best practices. By integrating these frameworks, Powerlink is committed to safeguarding its critical assets, personnel, and infrastructure.

This hybrid model enables Powerlink to:

1. **Keep our people safe and ensure Resilience**: By following the PSPF, Powerlink strengthens its capacity to prevent, detect, and respond to security threats, safeguarding operations against a broad spectrum of risks, including personnel risks, physical security hazards, and natural disasters.
2. **Protect Critical Infrastructure**: The ENA's framework helps focus on the protection of electrical infrastructure from potential threats, including terrorism, sabotage, and vandalism, ensuring continued delivery of safe and reliable energy to communities.
3. **Set Compliance and Governance Outcomes**: Adopting these frameworks ensures that Powerlink adheres to government regulations, security standards, and industry guidelines, promoting a culture of security and compliance across the organisation.
4. **Integrated Risk Management**: The hybrid approach promotes an integrated security and risk management strategy that addresses both immediate security challenges and long-term resilience objectives, ensuring that Powerlink is prepared for any emerging threats.

By blending the PSPF's broad policy guidelines with the specific industry context provided by the ENA and SOCI requirements, Powerlink ensures that its protective security strategy is both comprehensive and tailored to the unique risks and challenges associated with electrical infrastructure.

The *Security of Critical Infrastructure Act 2018* (SOCI Act), as amended in 2021 and 2022, is Australian legislation designed to strengthen the resilience and security of Australia's critical infrastructure across key sectors, including electricity, gas, water, communications, and others. The SOCI Act aims to protect these assets from both physical and cyber threats by imposing a range of obligations.

Entities involved in the generation, transmission, distribution, or market operation of electricity that are deemed of national significance fall under the scope of the SOCI Act. The legislation defines these entities as managing "critical infrastructure assets" and may designate some as "systems of national significance" (SoNS), requiring even more stringent oversight.

2.1.2 Security-in Depth

Security-in-Depth is at the core of the Protective Security approach. It refers to the integration of all facets of protective security into a tiered Protective Security approach, inclusive of multiple 'layers' of protection, as articulated in **Figure 4** below. Powerlink's security-in-depth physical security controls progressively harden a target by strengthening measures designed to deter, detect, delay, respond to and/or recover from a security incident or event, making an asset more resilient to loss, degradation, failure or compromise.

The Principles of Security-in-Depth are outlined below:

- **Deter**: developing a highly visible, overt security posture consisting of administrative, operational, physical and electronic security measures designed to deter potential threats from either planning or executing an attack.
- **Detect**: planning and implementing a combination of justified, scalable and proportionate security measures aimed at detecting a threat in planning or attempting to execute an attack
- **Delay**: planning and implementing physical security measures that delay (or deny) a threat the ability to physically access an asset, whilst allowing the response sufficient time to intercept the threat prior to the achievement of their objectives
- **Respond**: investing in the use of competent and well-resourced Police and Security personnel at following pre-defined security response plans and procedures effective at limiting a threat actors' chances of achieving their objectives
- **Recover**: investing in the development, exercising and testing of contingency plans that clearly articulate each step of the recovery process and strengthen our resilience for the organisation to security threats and other forms of disruption

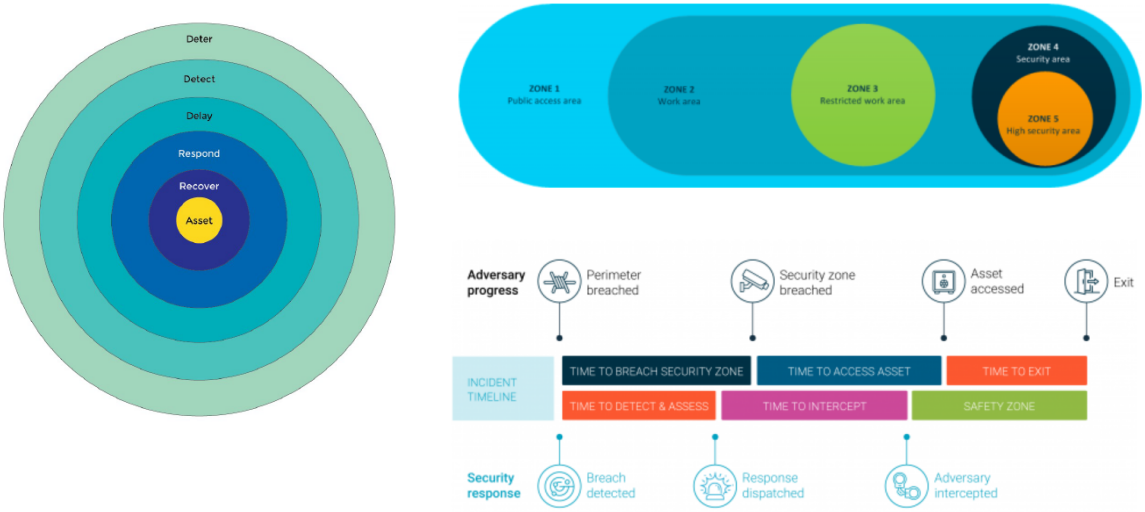
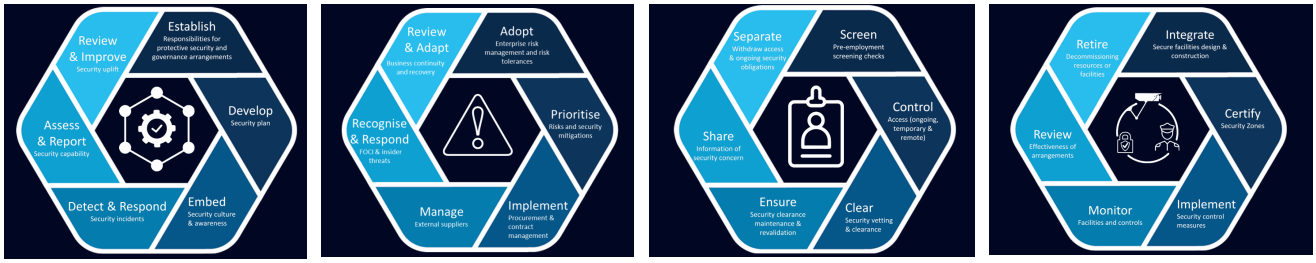


Figure 4 – Security in depth principles and critical path to unauthorised entry & response



2.2 Alignment to Strategic Objectives

2.2.1 Drive Value for Customers

Drive value for customers by ensuring a secure and supported workforce, enabling employees to work without fear of harm, and ensuring the continuity of service. Key elements like 24/7 monitoring, real-time situational assistance, and proactive risk management create a dependable and resilient organisation that can operate efficiently and securely, ultimately benefiting customers.

2.2.2 Unleash our Potential

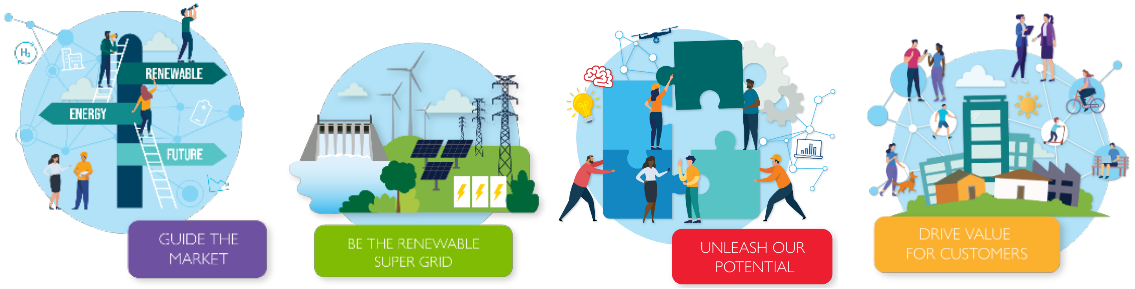
The Protective Security team will enable our people to unleash their full potential by delivering best-in-class physical security controls that minimise harm, protect critical assets, and foster a safe and resilient working environment. Through effective physical security measures, robust processes, and fit-for-purpose tools, we will ensure a high level of control effectiveness. Our proactive, risk-based approach will support our teams - anywhere, anytime - empowering them to focus on delivering exceptional outcomes for our customers and the communities we serve.

2.2.3 Guide the Market

The security strategy aligns with this goal by helping the company navigate industry challenges in a secure and risk-managed way, especially as it plays a leadership role in the energy sector. By establishing robust security standards, proactive intelligence-led alerts, and collaborating with external agencies, the strategy ensures that the company remains a trusted advisor to industry players and regulators, particularly in the face of the energy transition.

2.2.4 Be the Renewable Super Grid

Physical security is a critical part of supporting large-scale renewable energy projects and connecting them to the grid. The strategy ensures that physical security measures are in place across the entire business, protecting critical infrastructure and enabling smooth and secure integration of renewable energy sources. With initiatives like the centralised Protective security function, secure monitoring of assets, and responsive support for field operations, the strategy directly facilitates the company's renewable grid goals by maintaining operational integrity and ensuring staff are protected on the move.



3. Context and Interdependencies

3.1 Critical Infrastructure

Powerlink is a critical energy provider under the *Security of Critical Infrastructure Act 2018 (Act).* The Act requires that owners of critical infrastructure assets implement a risk management plan to mitigates material risks associated with cyber and information hazards, personnel hazards, supply chain hazards, and physical and natural hazards.

As an owner and operator of critical energy infrastructure in Queensland, Powerlink recognises the important role it plays in delivering essential services. Powerlink operates in a highly regulated environment and complies with a number of existing legislative and regulatory requirements that align to the intent of the Security of Critical Infrastructure Act 2018 (SOCI)

There are several Powerlink assets requiring a strong physical security posture as they deliver services to other essential services that would have adverse effects on the communities we serve.

The Critical Infrastructure Resilience Strategy sets out the Australian Government's joint business government approach to improving risk management, management of strategic issues and organisational resilience for owners of critical infrastructure. The two objectives of the Strategy are:

a) for critical infrastructure owners and operators to be effective in managing reasonably foreseeable risks to the continuity of their operations, through a mature, risk-based approach; and
b) for critical infrastructure owners and operators to be effective in managing unforeseen risks to the continuity of their operations through an organisational resilience approach. Powerlink participates in the Trusted Information Sharing Network (TISN) for the energy sector.

The Australian Department of Home Affairs has implemented regulatory reforms across the country through the Security Legislation Amendment (Critical Infrastructure) Bill 2022. As a result, Powerlink is obliged to comply with a series of Rules associated with the protection of electrical infrastructure assets deemed ‘Critical’ by the Australian Government.

3.1.1 Current State, Trends and Influences

In planning the approach to Protective Security and the interdependencies, it is important to understand the landscape in which Powerlink operates both in terms of Queensland as well as nationally, as part of the energy sector. In Queensland, significant investment is being made to provide secure and affordable electricity supply to the community at a time when Australia’s energy markets are facing significant challenges relating to electricity and gas prices, system security, gas availability, and energy and climate policy.

Energy transmission businesses are seeking to adapt to a range of market forces and disruptors including:

- Transitioning to a low-carbon energy sector (QLD target - 50% renewables by 2030);
- Diversified renewable energy, including storage options;
- Existing infrastructure investment;
- National climate and energy policy stability and integration;
- Demand management and efficiency planning will lead to transformed business operating models and the development of “home solutions;”
- Power generation – eg. reduced reliance on coal fired generation with greater reliance of gas fired generation to support peak demand; and
- Data collection, energy usage patterns and analysis will increasingly drive business and network activity.

3.1.2 Security of Critical Infrastructure Act (SoCI)

As an owner and operator of critical energy infrastructure in Queensland, Powerlink recognises the important role it plays in delivering essential services. Powerlink operates in a highly regulated environment and complies with a

number of existing legislative and regulatory requirements that will need to align to the intent of the *Security of Critical Infrastructure Act 2018* (**SOCI**)

Our strategy is designed to effectively manage the risks and ensure secure, safe and reliable supply of energy. Our strategy has been developed in a way that meets our obligations outlined in the *Security Legislation Amendment (Critical Infrastructure) Bill 2020.*

Rule 11 (1) (b) of *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* requires Powerlink to minimise or eliminate a material risk associated with a physical security hazard on a physical critical component and a natural hazard on the critical infrastructure asset.

Powerlink is currently undertaking a physical security assessment of critical sites to assess the physical security threats and vulnerabilities and recommend treatment options to reduce the physical security hazards. Into the future, physical security assessments will need to be conducted on critical sites annually. The remaining sites conducted every two years.

The assessments will be conducted by the Protective Security Team and include a physical inspection, audit and testing of the site security controls to determine the operational condition and effectiveness of the existing physical security measures.

It is fair to say that Powerlink's ability to meet effectively deter, respond to and control and restrict access to critical sub components requires determined focus to uplift our capability in this area.

There is a need to ensure our physical security measures are compared with acceptable minimum-security standards that offer a high degree of deterrence, early detection from unauthorised access, delay from increased resistance to forcible attack coupled with a security response capability.

The standards Powerlink need to align with stem from the Energy Networks Australia (ENA) guideline for protective security of electrical networks and the Australian Government protective security policy framework (PSPF).

This approach applies security-in-depth principles to progressively harden critical components with physical security measures that include fencing, vehicle barriers, pedestrian barriers, architectural security elements, lighting, signage, and electronic security measures.

Perimeter and building access control is a fundamental element of the physical security measures. Where practicable critical components are compartmentalised with access control to provide an additional layer of security.

Video surveillance is crucial to centrally monitoring critical sites, detecting unauthorised access, coordinating a response, and investigating security incidents, the need to implement a centralised control room has been recognised and underway.

Future state will see the Protective Security Team Lead, Operations and Governance responsible for ensuring measures are fully implemented, tested and reviewed. Further activities to be performed by the Protective Security Team include cyclic reviews/assessments, conducting investigations, compliance reporting and actions management.

Protective security planning must include measures such as site access controls, perimeter security, surveillance systems, and emergency response protocols.

To safeguard the business and meet SoCI obligations, the Protective Security team will implement several key measures as part of a broader strategy:

- **Enhance Security Awareness and Culture -** Foster a strong security culture within our teams by providing ongoing training and awareness programs, ensuring all staff are vigilant and understand security protocols.

- **Control and Restrict Access -** Implement enhanced physical security measures in critical areas of our facilities to control and limit access, ensuring individuals are recorded as entering our facilities as individuals with identity verification and that only authorised personnel can enter security sensitive areas once granted approval to do so.

- **Improve Governance of Identity and Access -** Strengthen identity and access management protocols to better manage who is accessing our facilities, ensuring compliance with security policies and minimising unauthorised entry.

- **Real-Time Threat Detection and Response -** Implement advanced monitoring systems for real-time detection of security threats, allowing for swift response to potential risks and minimising impact.

- **Design Out Opportunities for Crime -** Apply crime prevention strategies to our facility's design, reducing the likelihood of criminal activity by addressing vulnerabilities before they can be exploited.

- **Apply Crime Prevention Through Environmental Design (CPTED) -** Incorporate CPTED principles into the physical design of our facilities, such as improving lighting, landscaping, facility hardening, and access control to reduce opportunities for crime and enhance overall physical security.

3.2 Security of Supply

Australia's critical infrastructure is regulated through Commonwealth, and state and territory legislation. These legislative and regulatory settings are augmented by industry codes of practice, as well as emergency management arrangements. For example, in the event of emergencies, the Australian Government Crisis Management Framework (AGCMF), the National Coordination Mechanism (NCM) and long-standing state and territory emergency and crisis management arrangements may be stood-up.

The increasingly interconnected nature of Australia's critical infrastructure exposes vulnerabilities that, if targeted, could result in significant consequences for the economy, security and sovereignty.

Such disruptions can create a chain of cascading consequences with profound effects on societies and communities, and interconnected infrastructure systems.

The impacts of unlawful interference can be long term, complex and have a cascading bearing on daily life and the social and economic wellbeing of communities. These events highlight the nation's reliance on our critical infrastructure, its interconnected systems, the challenges in maintaining it, and in some instances the fragility of systems such as supply chains and the workforce.

For example, a prolonged and widespread failure in the energy sector would have a nationally significant effect, such as:

- Impacts to water supply and sanitation, and in turn public health
- Reduced services or shutdown of the banking, finance and retail sectors
- Instability in the supply of food and groceries
- Disruptions to transport and telecommunications networks
- Impacts to delivery of health services and medical supplies
- Impacts to government and its services.

Powerlink provides high voltage electricity transmission network services, providing electricity to more than five million Queenslanders and 241,000 businesses including other critical infrastructure sectors such as Banking & finance, Health, Water Services, Communications, Food & Grocery, Transport and Energy which also included Oil & Gas, all covered under the SoCI legislative requirements.

With a significant and varied property and asset portfolio of both network and non-network sites it is essential to minimise any disruption and related impacts, so the continuity of supply is maintained to communities and businesses. This must be achieved safely for both the workforce and community whilst enabling service delivery to occur unhindered. The interdependencies and interconnectedness of the supply of electricity is illustrated below:

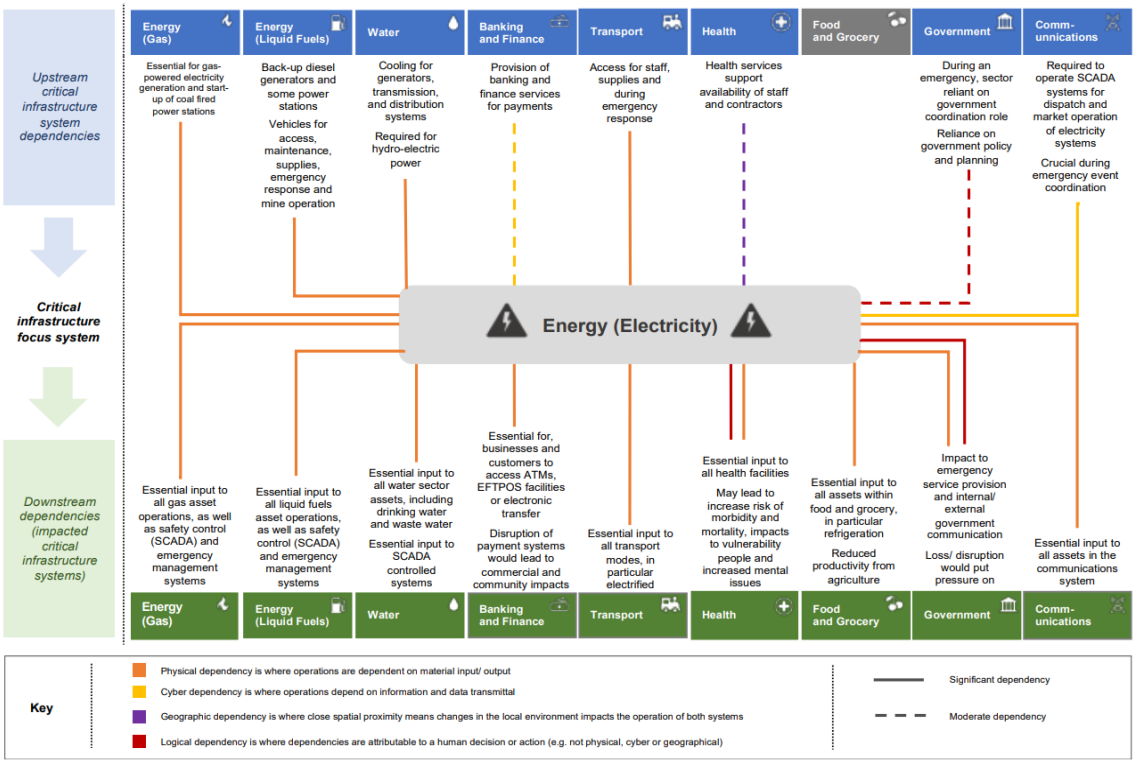


Figure 5 – Critical Infrastructure interdependencies

4. Security, Risks and Threats

4.1 2025-2030 ASIO National Threat Assessment

In February 2025, latest ASIO Annual Threat Assessment ASIO warned that Australia's security environment will become increasingly unpredictable and complex over the next five years. The country will face more dynamic and diverse threats, with the second half of the decade likely to bring more surprises. ASIO highlighted the growing risks of communal violence, espionage, foreign interference, and sabotage targeting Australia's Government, Defence and Critical Infrastructure. ASIO emphasised that Australia is confronting unprecedented challenges, with multiple threats intersecting at once, making the situation more dangerous than ever before.

Key foundations of Australia's security - like social cohesion, trust in institutions, and the truth itself - are being tested, with rising intolerance and the spread of misinformation. ASIO is already focused on three key threats: espionage, foreign interference, and politically motivated violence. The risk of terrorism is also increasing, with lone actors or small groups, often unknown to authorities, becoming a more significant concern. Interestingly, many of these incidents are not linked to overseas groups but are instead motivated by mixed ideologies, including nationalism and racism. (Source: ASIO National Threat Assessment)

4.2 Terrorism, Activism and Issue Motivated Groups

Australia's national security landscape has entered a period of heightened vulnerability, driven by a complex and volatile mix of social, political, and global factors. While individual threats in isolation may not pose immediate danger, the combination of these drivers is eroding the security environment in significant ways. Social cohesion is weakening, and public trust in government and democratic processes is declining, mirroring trends seen globally. The COVID-19 pandemic and the Israel–Hamas conflict have accelerated these shifts, destabilising social trust and further undermining institutional confidence.

Emerging security threats are diverse, with grievances and ideologies not previously encountered on a national scale. While traditional violent extremist ideologies such as extremism remain persistent threats, they are now accompanied by a broader spectrum of radicalised individual(s) motivated by a variety of grievances. Consequently, acts of political-motivated violence (PMV) are expected to increase, particularly within domestic environments.

The National Threat Advisory System supports owners and operators of critical infrastructure to secure their assets, however, not all threats have implications to critical infrastructure.

Australia's general terrorism threat level is **PROBABLE** - there is a greater than fifty per cent chance of an onshore attack or attack planning in the next twelve months.

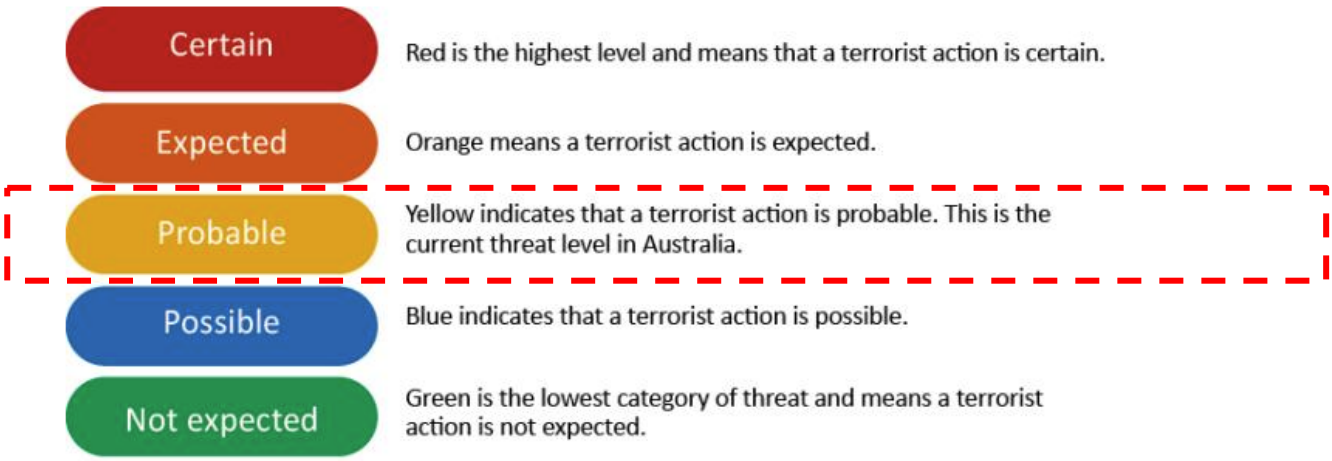


Figure 6 – Definitions of the 5-tiered National Terrorism Threat Advisory System

Queensland's strategic counter-terrorism arrangements are led by the Queensland Security Committee comprised of leaders and officials to ensure whole-of-government coordination and leadership.

An assessment of the attack vectors suggests that a terrorist attack in Australia is most likely to be low-cost, locally financed and of low complexity such as:

• carried out by an individual or small group; and

• employ simple tactics and using basic weapons (e.g. knives / vehicle ramming), firearms and/or improvised explosive devices (IEDs).

More complex types of attacks are less likely but cannot be ruled out.

4.3 Security Risks

It is important for protective security arrangements to be considered based on a risk-based approach utilising advice from law enforcement and intelligence agencies but in the local context of the security situation. To enable effective communication and support, the Protective Security team cultivate and maintain relationships with law enforcement and intelligence agencies. The benefits to Powerlink include but are not limited to early notification and assessment of threats as well as advice surrounding effective mitigation measures.

The table is an example of the types of security hazards and risks Powerlink faces as well as the types of incident they might lead to which would require Protective Security involvement:

SECURITY HAZARD	SECURITY RISK	TYPE(S) OF SECURITY INCIDENT
CRIME	Theft	• Petty / Opportunistic - Copper • Burglary • Organised Crime
	Malicious Damage	• Vandalism • Damage to buildings and equipment • Damage to vehicles
	Violence / Assault	• Physical Assault • Sexual Assault • Harassment / Intimidation
	Fraud	• Funding misappropriation • Corruption • Fraudulent/unauthorised use of resources
	Threats / Hoaxes	• Telephone, email, social media bomb threats • Hoax letters • Hoax bombs / suspect items/White powder
SECURITY HAZARD	**SECURITY RISK**	**TYPE(S) OF SECURITY INCIDENT**
PROTEST	Direct Protest	• Protest or demonstration • Riot • Blockade • Chaining to plant/equipment • Placing foreign locks
	Indirect Protest	
SECURITY HAZARD	**SECURITY RISK**	**TYPE(S) OF SECURITY INCIDENT**
TERRORISM	Direct Terrorism	• Improvised Explosive Device (placed at site) • Improvised Explosive Device (suicide bomber) • Improvised Explosive Device (vehicle borne) • Attack with firearms / edged weapons • Mixed mode (combination of weapons / tactics) • Vehicle ramming / Hostile vehicle • Attack with chemical, biological or radiological agents • Letter / parcel bombs

4.4 Future State – Trends, Influences & Challenges

4.4.1 2032 Olympics

The Brisbane 2032 Olympics will necessitate significant security enhancements to address the expected international spotlight and the associated elevated risk of sabotage, unauthorised interference, and other potential threats. With thousands of spectators, athletes, officials, and media attending, the city's infrastructure, particularly the transmission network, will be under intense scrutiny from a power system security and reliability of supply perspective supporting critical functions such as transportation, law enforcement/security, broadcasting, operations, and healthcare. Recent International events have shown a desire to sabotage or use critical infrastructure for extremist purposes. Given the rising risks in the global security landscape, high-profile events like the Olympics have increasingly become targets for a range of threat actors using diverse methods and motives.

4.4.2 Landowner and Community Engagement

True landowner and community engagement presents challenges with mixed views within the community. Moreover, the rise of the sovereign citizen movement, compounded by the societal disruptions of the COVID-19 pandemic and increasing distrust within the community has amplified resistance to large scale projects, both in metropolitan and regional areas.

The sovereign citizen movement, which rejects government authority and promotes individual autonomy, has cultivated an environment where infrastructure projects requiring land access can be seen as government overreach. The pandemic only deepened this distrust, as many felt the government's response was overbearing or mismanaged. For landowners and communities already wary of government intervention, these factors create an atmosphere of heightened opposition to energy projects that might otherwise be considered. This combination of distrust, ideological resistance, and competing infrastructure projects has created a challenging landscape for energy developers, who now must navigate not only logistical and technical hurdles but also a deeply divided social and political context.

4.4.3 Ongoing alignment of Physical Security to Prevent Cyber

The evolving threat landscape demands a more collaborative and integrated approach between cyber and physical security disciplines. While cyber threats have justifiably received significant attention, this emphasis has inadvertently created a disproportionate focus that risks neglecting other critical vulnerabilities - particularly those related to physical breaches, insider threats, and the convergence of these risks.
In the next five years, the security environment is expected to further deteriorate, with increasing challenges posed by espionage, sabotage, politically motivated violence, and insider-driven attacks. As adversaries encounter more robust cyber defences, they are likely to pivot towards exploiting gaps in physical security and human factors - often the path of least resistance.

To counter these risks, it is essential that physical security systems, such as access control, surveillance, and intrusion detection, are not only seen as protective measures but also as intelligence assets capable of identifying indicators of compromise relevant to cybersecurity.

For example, unauthorised physical access may be a precursor to data exfiltration or manipulation of critical operational technology systems.

An effective defence strategy must therefore move beyond siloed risk management. In line with the "All-Hazards" approach mandated by the *Security of Critical Infrastructure Act 2018* (SOCI Act), this strategy emphasises the need for a unified security posture. This includes:

- Cross-domain threat modelling that recognises the interdependencies between cyber, physical, personnel, and supply chain risks.
- Coordinated incident response planning to address blended threats that span both physical and digital environments.
- Shared intelligence and monitoring platforms to ensure early detection and coordinated response to emerging threats.

The activities within this strategy aim to embed this integrated security mindset across the organisation. By recognising and operationalising the interconnectivity of all threat vectors, we will strengthen our overall resilience and ensure that our critical infrastructure is safeguarded against both current and emerging threats.

4.4.4 Legislative Enhancements

As the security landscape continues to evolve and regulatory bodies recognise the increasing complexity in addressing material risk, it is imperative that we assess and adapt our existing legislation and risk frameworks to ensure their effectiveness. Our strategy must remain flexible, allowing for quick pivots in response to the unpredictable nature of the diverse and growing range of security threats to our business. By fostering adaptability, we will mitigate potential risks and safeguard the long-term stability and integrity of our operations.

5. Security Health Check / Culture

The setting of a security culture requires a top-down approach to embed the values, attitudes and behaviours which are foundational to the effectiveness of Protective Security. The required cultural shift at every level of the corporation can be achieved by the following:

- Powerlink Risk Appetite Statement;
- Engagement and consultation across all areas led by EGMs, GMs, regional and project managers and those with a leadership role;
- Increased awareness to understand the benefit of timely and consistent reporting of incidents, including to security and law enforcement authorities as appropriate;
- Increased support to champion ‘ethics’ in security behaviours and awareness, for example the visible displaying access passes and reporting of security concerns;
- Refreshed security communications to maximise audience attention and retention of the key facts, including improved learning content;
- Tailoring the security message delivered to work group types so they can relate it to their work area(s) and how security breaches affect everyone;
- Proactive involvement with asset management and investment so enterprise security solutions are optimised, and appropriate Lifecycle Planning undertaken;
- Improved engagement with business change management initiatives during business case development so that Security by Design principles are adopted, and funds identified within the project scope(s); and
- Continuous improvement surrounding the delivery of efficient and effective physical security service including the utilisation of technological advances.

5.1 Security Culture - Current State

The current state of the Protective Security within the business is characterised by several key issues:

- **Siloed Approach**: Physical security efforts are fragmented and lack coordination across different departments or business areas.
- **Inconsistent Hardware Deployment**: There is no uniform strategy or standard for deploying security hardware across the organization.
- **Low Physical Security Culture**: Employees and stakeholders are not fully engaged or educated on physical security best practices.
- **Sporadic Incident Reporting**: There is limited reporting (frequency and detail) of physical security incidents, which hampers response and improvement efforts.
- **Limited Enterprise-Wide View**: The organisation lacks a centralised view of physical security incidents and data, limiting its ability to assess risk and take proactive measures.
- **Absence of Real-Time Awareness**: The business does not have systems in place for real-time monitoring or awareness of security situations.

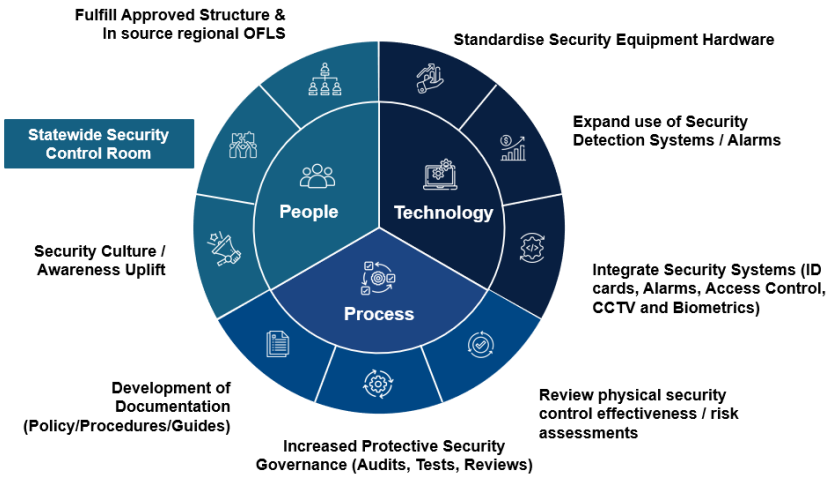
- **Weak Response Capacity**: There is a reduced ability to deter, detect, and respond effectively to physical security threats.
- **Lack of Governance/Engagement**: There is no formal governance or engagement framework for physical security, leading to a lack of accountability and strategic direction.
- **Low Maturity**: The business has low maturity in terms of physical security controls and their effectiveness, indicating that security systems and practices need significant improvement.

In summary, the business's Protective Security posture is reactive, inconsistent, and underdeveloped, with major gaps in security incident management, response capabilities, and protective security culture.

5.2 Physical Security Culture - Future State

We aim to be a leading protective security team that instils unwavering confidence in our people, ensuring they know they have the full support needed to perform their work anywhere, anytime, without fear of harm. Our vision includes:

- Expanding on our contracted guard force services to operate a **24/7 Enterprise Security Control Room** for continuous monitoring and support
- A **centralised security function** that integrates security across the entire business
- The **design of robust physical security standards and consistent hardware** to ensure reliability
- **Robust** and effective, **risk-based security controls**
- **Real-time situational monitoring and assistance**, providing immediate response to any security needs
- **Dedicated field and travel support** to assist staff on the move through our Security Control Room
- The establishment of a **Security Working Group** to collaborate with internal teams and critical infrastructure organisations, law enforcement and intelligence agencies
- **Annual refresher training** to keep security practices sharp and current
- The **creation of comprehensive physical security standards, policies, and procedures** to ensure uniform protection
- A continued focus on **driving value for customers**, aligning security operations with business objectives
- A **collaborative approach with** internal, external and law enforcement / intelligence **stakeholders**



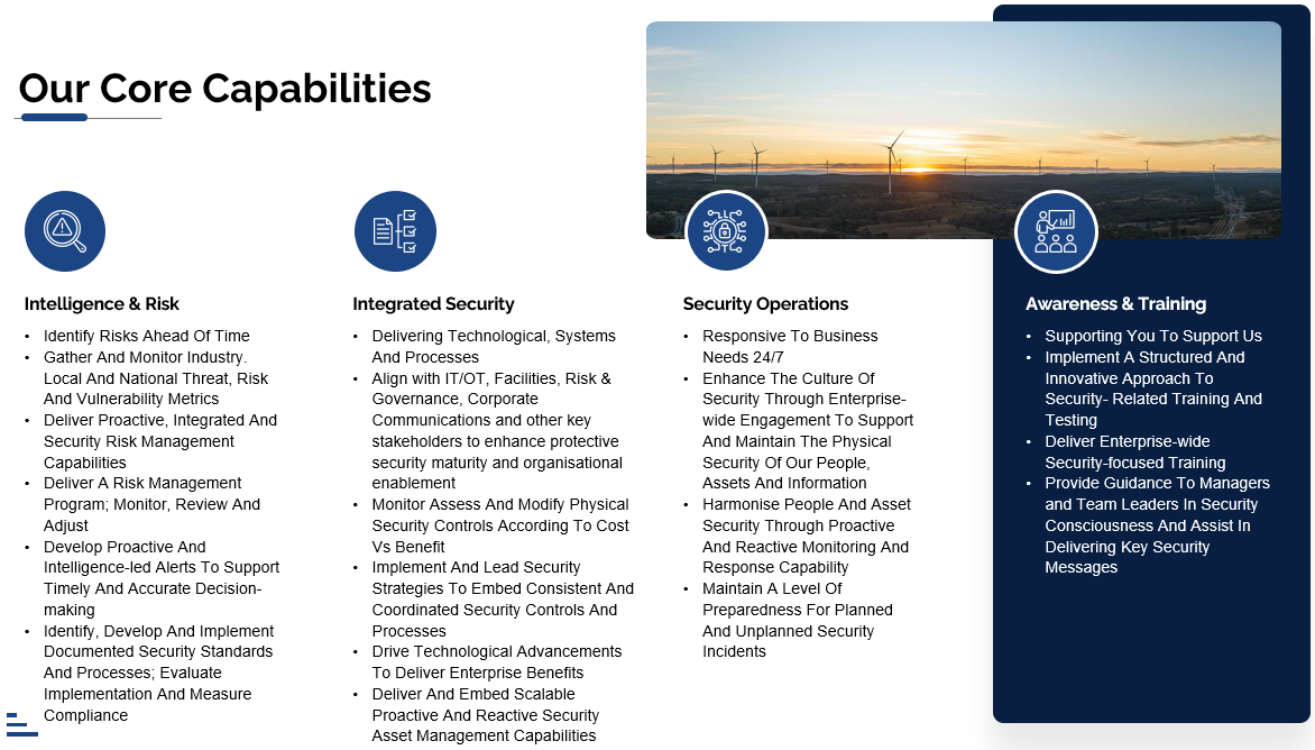
Integrated Approach to Keeping Us Safe

Essential components	Protective Security Actions/Outputs
Know the threat to our workplace and prepare accordingly	• Develop a substation risk and maturity assessment. • Conduct risk assessments to identify unique risks and risk tolerance. • Apply a risk-based approach to security: focus attention and resources where it will achieve the best outcomes.
Develop a physical security plan and establish a working group responsible for engagement and collaboration on physical security matters	• Develop a security plan and establish a working group responsible for engagement and collaboration on security matters and decision-making. • Establish sound and tested policies and procedures that are easy to follow and access. • Review policies and procedures to manage any risks posed by external visitors, contractors, managed service providers, staff working remotely and staff travelling overseas.
Build a strong security culture to enable, encourage and educate employees	• Regularly assess the culture for trends that require attention. **Enable**: leadership, compliance and correction. **Encourage**: ownership, reporting, discipline, innovation and confidence. **Educate:** communicate and deliver security awareness training to all staff.
Install and maintain physical security systems to protect people, places, technology and information (Deter, Detect, Delay, Respond)	• Provide secure and reliable infrastructure design standards (as part of a revised Asset (Security) Management Strategy. • Ensure security sensitive areas (SoCI declared) have systems that are auditable and can control access to sensitive information and assets, detect breaches or attempted breaches of access and provide real-time alerts about unauthorised access to a centralised, enterprise security support centre. • Standardise, risk-based approach to physical security standards for operational and non-operational standards.
Real time visibility and awareness on threats / incidents and response **(Security Control Room)**	• Design and implementation of a dedicated, whole of business security control room. Protecting our people and assets in real time, intelligence led decision making. The Security Control Room will work to deter criminal activity, detect abnormal events, and instigate an immediate response from a work class security support centre giving our people access to best in class support and our assets the level of protection required to ensure we continue to deliver essential services to our community and customers.
Recognise and respond to suspicious behaviour and security incidents	• Establish a reporting mechanism that is confidential, accessible and timely. Educate employees on what to report and how, ensuring ease of reporting in the field. • Recruit and train security control room officers to recognise and respond to possible reconnaissance activities. • Establish emergency and security incident investigation and response procedures (Site Security Plans).
Regularly review controls for effectiveness	• Undertaking a review of existing security governance and controls. Undertake ongoing security assessments of site (upon recruitment) and establish security controls testing framework. • Reviewing security incidents to assess if there were missed opportunities to intervene earlier. • Review and test incident response and investigation procedures for effectiveness

Engage with law enforcement/intelligence & other CI operators	• Lead collaboration by driving collaboration, partnerships and forums on critical infrastructure protection not only lift the capability of PQL but to share our knowledge and experience across other industry sectors.

6. Focus Areas, Actions and Engagement

There are four (4) core capabilities which form the basis of our approach.



6.1 Core Deliverables to Uplift Our Security Maturity

Solutions are rarely 'one size fits all,' and the programme of works will be delivered on a risk-based approach. The effectiveness of the Protective Security strategy, associated initiatives and program of works will require Executive level commitment to embed the values and make security part of everyone's responsibility. Consequently, the uplift will be delivered over several years.

6.1.1 Security Control Room

The establishment of a 24-hour security control room is a key priority in Powerlink's protective security strategy, as it addresses the current lack of a centralised location for monitoring and responding to security incidents across all components of the business. As the operator of Queensland's high-voltage electricity transmission network, Powerlink is responsible for securing critical infrastructure, requiring an efficient and effective framework for detecting and managing both local and off-site threats. The proposed control room will serve as a centralised hub, enhancing the company's ability to monitor physical security risks, safeguard personnel, and protect assets and operations in real-time.

Additionally, amendments to the Security of Critical Infrastructure (SOCI) Act have introduced stricter regulations that mandate comprehensive risk management programs. The security control room is a vital step in ensuring Powerlink meets these compliance obligations and enhances its security framework. By providing a real-time,

centralised monitoring capability, the control room will improve situational awareness, strengthen incident management, and help Powerlink fulfill its legal and operational security responsibilities under the SOCI Act.

6.1.2 Landowner and Community Relations Safety Enhancements

Continuing collaboration with the landowner and community relations teams to identify opportunities for safeguarding individuals during field activities. This will ensure proper planning, risk mitigation, and informed decision-making to empower the team in fostering genuine engagement and building meaningful connections with the community. The strategy will include the development of safety and security procedures, the integration of effective technologies, and the provision of valuable training in adaptive communication for frontline staff, equipping them to handle challenging situations and navigate potentially risky circumstances safely.

(Note: this activity will also consider wider impacts to other field-based teams if/where required)

6.1.3 Physical Security Uplift to Sub Stations

As part of our security strategy to protect business-critical assets, a targeted risk assessment will be conducted to evaluate the criticality and vulnerability of each site. This process will ensure that implemented security controls are proportionate, effective, and aligned with our obligations under the Security of Critical Infrastructure (SoCI) Act. Controls must support our ability to restrict and manage access, enhance physical protection measures, and harden sites against potential threats. The overarching objective is to establish a layered security posture that deters criminal activity, enables early detection of unauthorised access or tampering, delays offenders from achieving their objectives, and facilitates a timely and coordinated response. This includes the strategic deployment of physical and technical security measures such as perimeter fencing, security signage, lighting, CCTV, access control systems, intruder detection, and hostile vehicle mitigation infrastructure.

6.1.4 Virginia and Primary Disaster Recovery Complex Security Enhancements

These facilities need an upgrade to physical security for several key reasons:

1. **Limited perimeter monitoring**: The current CCTV coverage is insufficient, and there's no detection capability at the perimeter fence.
2. **Ineffective reception area**: The reception is too busy to properly monitor all entry and exit points.
3. **Vulnerable perimeter**: The perimeter fence and gates are not strong enough to prevent unauthorised access, and tailgating into the facility is too easy with no detection capability.
4. **Slow vehicle gate response**: The vehicle gates take too long to close, increasing vulnerability.
5. **Inability to prevent forced entry (not hardening)** The areas have limited detection or physical barriers (layers) and the core barriers are chain wire fences with no detection and glass doors/windows.

The goal is to create a secure yet welcoming environment that protects the building, ensures safety, and prevents unauthorised access. The complex needs to detect security threats early, respond effectively to major security events, and ensure the protection of our people and a key facility.

6.1.5 Enhanced Use of CCTV

To strengthen our proactive threat detection and response posture, we will modernise our CCTV infrastructure, transitioning from a disparate and fragmented system to an integrated, enterprise-grade solution. This will include uplifting camera capability to enable automated detection, real-time alerting, and intelligent tracking of potential security threats - supporting effective triage and immediate operational response.

The new head-end CCTV system will incorporate advanced features such as Pan-Tilt-Zoom (PTZ), thermal imaging, loitering detection, and AI-powered analytics. These enhancements will significantly improve deterrence, support intelligence gathering (e.g. detecting criminal probing or planning activities), and provide enhanced situational awareness across our sites.

A centralised and dedicated Security Control Room will manage this infrastructure, ensuring robust governance, strict access control, and compliance with SoCI (Security of Critical Infrastructure) obligations. The solution will not only enhance our detection and response capabilities but also offer long-term cost efficiencies, reducing reliance on physical deterrents such as electrified fencing at lower-criticality sites. In addition, a key element of

the plan is the implementation of advanced mobile trailer technology, which will be equipped with CCTV cameras that are monitored in real time by the Powerlink security control room, ensuring effective surveillance and a higher level of site security and initiation of an effective response to remote/mobile sites.

6.2 Annual Roll Out Activities (12 month plan)

Powerlink strategies enable the functional groups to deliver strategic objectives and it is important the Protective Security initiatives complement our cross-functional business partners.

The following initiatives for the next 12 months are considered the foundation upon which further activity will be **identified and progressively delivered with the annual focus areas reviewed annually.**

1	Security Education and Compliance	Creation of a dedicated Protective Security, mandatory online module
2	Security Risk Assessment Program	The creation of a scheduled risk assessment program, ongoing for all sites.
3	Corporate Facility Infrastructure Security Program	A number of important business sites will receive security upgrades to deliver the basic fundamentals of visitor sign in, intruder detection and real time CCTV
4	Physical Security Key Review	Ensure robust key management procedures to adequately control access and provide further reliance on effective electronic access control – removing master keys from circulation
5	Protective Security Documentation – establishment of security procedures, standards and frameworks.	Protective Security is required to develop a suite of security documents to socialise with the business. These documents will be utilised by the business and available to external consultants/architects for construction activities. (Hardware, design, procedure)
6	Access Control (Site Entry) Standardisation Program	Focus on phasing out manual key entry to sub stations and achieving electronic access control entry / exit
7	Creation of a secondary Security Control Room	Ensure continuity of business wide security functions by way of a disaster recovery security control room
8	Implementation of Proactive International Travel Safety and Security Support system	Implementation of an itinerary based travel safety and security monitoring platform with a particular focus on international business travellers
9	Protective Security Governance Group	Establishment of Protective Security Governance Group
10	Creation of a Landowner Security and Safety Procedure	Work to a standardised way of planning, assessing and mitigating risk
11	Identification Card and Access Standardisation	Creation of an ID & Access standard for personnel, visitors, contractors and service contractors that ties in with a new Access Management Procedure

12	Improve access management arrangements, governance and review. Creation of an Access Management Procedure	Creation of an Access Management Procedure, workflow request portal with authorised custodians and access group reviews.
13	Improved Security Incident Reporting and Data Analysis	Enhanced and efficient security incident reporting – including an extension on electrical events to also include corporate security incidents
14	Creation of Facility Security Liaison Officer functions	The Facility Security Liaison Officer (FSO) initiative is a new program designed to enhance security awareness and resilience across our remote, staffed facilities. Under this initiative, an existing site representative will be nominated and equipped with targeted security training to serve as the primary liaison between the facility and the central security team. The FSO will act as the on-site security champion, promoting best practices, supporting incident response, and fostering a stronger security culture within their location. To support this role, an informative and practical training package is being developed to provide FSOs with the knowledge, tools, and confidence required to manage security-related matters effectively.
15	Introduction of Security K9 to Project Site for Lone Worker Protection	To strengthen the effectiveness of ad-hoc guarding at high-risk project sites, a revised security procedure is proposed. A critical priority will be to avoid placing lone security officers in high-risk settings. In accordance with the Queensland Security Providers Act, the strategy will also include the use of licensed security personnel supported by trained canines, enhancing deterrence and response capability across vulnerable locations.
16	Introduction of Biometrics to Security Enhanced Areas	The initiative aims to address the ongoing issues of card sharing and cloning by introducing biometric readers to restricted areas (Data Centres, Network Operations, Critical Sub Components areas as per SoCI and Security Control Room). This will strengthen access control, enhance security, and ensure compliance with AESCSF and Physical Security controls under the Security of Critical Infrastructure Act. Proper consultation and planning will be done prior to implementation. By adopting biometric access systems, we can ensure stricter control over who gains access to sensitive areas, minimising the risks of unauthorised entry through cloned or shared cards. This shift will not only improve the overall effectiveness of our access management systems but also provide greater alignment with governance requirements.

7. Collaboration with Industry, Police and intelligence Agencies

The Protective Security Team maintains ongoing relationships with the following groups to ensure effective collaboration with industry, government, policing, and intelligence agencies:

7.1.1 Statewide Police and Intelligence Agency Liaison

Lead and strengthen a strong partnership with Queensland Police (QPS) and the Australian Security Intelligence Agency (ASIO) is essential to improve our security response and support. By fostering a deeper understanding of our business, operations, and critical infrastructure sites, we can ensure greater awareness within police patrol response zones and proactive threat information. This initiative will focus on sharing insights into incident trends, our role as a provider of essential services, and the unique challenges we face. In turn, this collaboration will enhance proactive patrols, streamline responses to events, and provide faster, more effective support during calls for service. Ultimately, this two-way relationship will lead to more efficient and successful outcomes in securing our sites and ensuring community safety.

7.1.2 Queensland Critical Infrastructure Working Group

The Queensland Critical Infrastructure Working Group for Copper Theft (referred to as the “Working Group”) has been re-established to address the growing issue of copper theft and its impact on critical infrastructure across Queensland. Copper theft poses significant risks to community safety, the operational integrity of vital infrastructure, and sectors such as telecommunications, power, and transportation.

The Working Group's mission is to foster cross-sector collaboration to identify challenges, share information, and develop coordinated strategies to mitigate copper theft and its consequences.

Objectives

The key objectives of the Working Group are:

- To provide a forum for stakeholders to discuss copper theft and its impact on critical infrastructure.
- To improve coordination and collaboration among law enforcement, infrastructure providers, government agencies, and other key stakeholders.
- To identify trends, vulnerabilities, and best practices in preventing and responding to copper theft.
- To develop and implement strategies, policies, and initiatives aimed at reducing copper theft, and advocate for legislative amendments at the State and Federal levels.
- To enhance the reporting and tracking of copper theft incidents.
- To raise community awareness about the risks and consequences of copper theft.

7.1.3 Trusted Information Sharing Network (TISN)

The Trusted Information Sharing Network (TISN) is a platform where industry and government work together to enhance the security and resilience of critical infrastructure. Through TISN, members of the critical infrastructure community collaborate to strengthen their organisations and industry sectors against all hazards.

Key objectives of TISN members include:

- Identifying and managing risks to critical infrastructure.
- Addressing security gaps within sectors and implementing mitigation strategies.
- Informing policy and programs that support critical infrastructure resilience.
- Achieving the objectives of the Critical Infrastructure Resilience Strategy.

7.1.4 Critical Infrastructure Centre (CIC)

In January 2017, the Commonwealth Government established the **Critical Infrastructure Centre (CIC)** to safeguard Australian critical infrastructure from national security risks such as sabotage, espionage, and coercion.

The CIC leverages Commonwealth Government expertise to help owners and operators better understand and manage risks, as well as build resilience. The CIC offers risk assessments and advice on managing threats from malicious actors.

The Security of Critical Infrastructure Act 2018 formalised the management and oversight of national security risks related to foreign involvement in Australia's critical infrastructure, covering electricity, water, gas, and ports.

7.1.5 Other Working Groups and Key Stakeholders

- National Transmission Security Leaders Security Working Group (Chair)
- Copper Theft and Sabotage Working Group
- QLD Police Counter-Terrorism Unit
- Department of Home Affairs
- Energy Networks Australia (ENA) – Physical Security Standards

8. Protective Security Personnel and Resourcing

8.1 Establishment of the Protective Security Team (Organisational Alignment and Improvement)

The Protective Security team was established in August 2024 with the appointment of the Manager, Protective Security and the amalgamation of the Officer for Local Security within the Southern region and shortly after this, the Northern and Central regional Officer for Local Security, currently an outsourced function, undertaken by Ergon. The Team Leaders were appointed in December 2024.

8.2 Appointment of Physical Security Resourcing

To achieve a consistent, enterprise-wide physical security capability, the executive-endorsed organisational structure for the Protective Security function - approved in April 2024 - provides a clear pathway to maturity. However, several key vacancies remain unfilled, limiting our ability to deliver on priority security initiatives at pace.

The desired end state will comprise trusted business specialists with deep expertise across protective security operations, including real-time security advice, standards and compliance, travel security, physical systems oversight, investigations, and risk management. These roles are essential in embedding a proactive and coordinated security posture across the business.

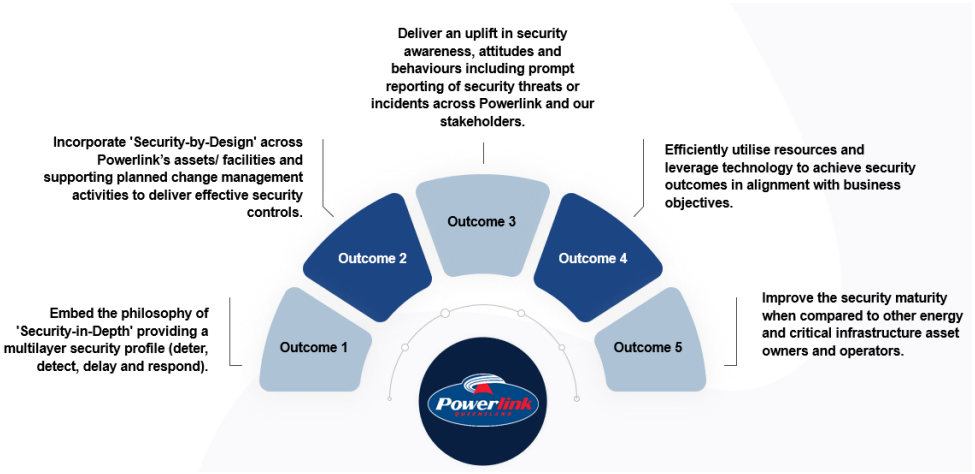
A key opportunity for uplift lies in transitioning from the current fragmented arrangements - particularly in the Central and North regions where Officers for Local Security (OFLS) are presently managed by Ergon - towards a fully integrated, statewide model. This transition will involve the creation of dedicated regional Physical Security Advisor roles, along with consolidated responsibility for the OFLS and Electrical Authorisations functions under a single, unified Protective Security umbrella.

Moving away from the existing ad-hoc and shared resourcing model with Ergon is key to achieving an all of business physical security overlay and support structure. A dedicated, properly resourced physical security function will support consistent application of controls, strengthen external partnerships (including with Queensland Police and Major Service Partners), and elevate the security culture across the organisation.

9. What Success Looks Like

Our strategy identifies the following outcomes to be achieved, or desired end-state, so that we can determine whether our strategy is successful. These are as follows:

- **Outcome 1 - Embed the philosophy of 'Security-in-Depth'** providing a multilayer physical security profile (deter, detect, delay and respond);
- **Outcome 2 - Incorporate 'Security-by-Design'** across assets / facilities and supporting planned change management activities to deliver baseline security controls across the Powerlink portfolio;
- **Outcome 3 - Deliver an uplift in security awareness**, attitudes and behaviours including prompt reporting of physical security threats or incidents across Powerlink and our stakeholders;
- **Outcome 4 - Efficiently utilise resources and leverage technology** to achieve security outcomes in alignment with business objectives, including a reduction in theft, unauthorised access to Powerlink sites and increased rate of prosecution; and
- **Outcome 5 - Improve the overall Protective Security maturity** when compared to other energy and critical infrastructure asset owners and operators.



On an annual basis, Powerlink release strategies and plans to enable the functional groups to deliver the strategic objectives and it is important that the Protective Security key initiatives and outcomes complement the activity of our cross-functional business partners.

An overview of our strategy is provided at Appendix A.

10. Distribution List

Divisional Distribution	Contact details
Chief Executive	Chief Executive
People and Corporate Services	General Manager People and Culture
Delivery and Technical Solutions	General Manager, Infrastructure Delivery
Finance and Governance	Manager, Governance, Risk and Insurance
People and Corporate Services	Manager, Commercial Property Portfolio
Major Projects	General Manager, Major Projects Delivery
Network and Business Development	General Manager Network Portfolio
Group/Team Distribution	Contact details
Corporate Communications	Manager Internal Communications
Network Operations	General Manager, Real Time Network Operations
Network Operations	Manager Network Performance
Asset Strategies	Manager, Asset Strategies
Business IT and Digital Delivery	GM Business IT & Digital Delivery
Health and Wellbeing	Manager, Health and Wellbeing
Community and Delivery Services	General Manager Community and Delivery Services
Enterprise Resilience	Manager, Enterprise Resilience

Appendix A. Protective Security Overview

Protective Security Overview

OUR PURPOSE
Connecting Queenslanders to a world-class energy future.

OUR VALUES
Our values guide our decision- making and underpin the way we support our purpose and strategic objectives - guide the market, be the renewable super grid, drive value for customers, and unleash our potential.

OUR STRATEGIC OBJECTIVES

- Enabling Diversity of generation & storage
- Supporting industry and load growth
- Working with stakeholders to ensure a cost-effective, reliable and safe supply
- Develop grid technologies to manage future network

PROTECTIVE SECURITY CORE BELIEF
Protective Security is a business enabler keeping our people and assets safe and secure

PROTECTIVE SECURITY FUNDAMENTAL OBJECTIVE
To partner with the business to anticipate, prepare and respond to adverse events, minimizing frequency and severity

OUR CORE CAPABILITIES

INTELLIGENCE & RISK
- Identify risks ahead of time
- Gather and monitor industry, local and national threat, risk and vulnerability metrics
- Deliver proactive, integrated and security risk management capabilities
- Deliver a risk management program; monitor, review and adjust
- Develop proactive and intelligence-led alerts to support timely and accurate decision-making
- Identify, develop and implement documented security standards and processes; evaluate implementation and measure compliance

INTEGRATED SECURITY
- Delivering technological, systems and processes
- Lead the alignment in IT/OT, Facilities, Risk & Governance, Corporate Communications and other key stakeholders to enhance protective security maturity and organisational enablement
- Monitor assess and modify physical security controls according to cost vs benefit
- Implement and lead security strategies to embed consistent and coordinated security controls and processes
- Drive technological advancements to deliver enterprise benefits
- Deliver and embed scalable proactive and reactive security asset management capabilities

SECURITY OPERATIONS
- Responsive to business needs 24/7
- Enhance the culture of security through enterprise-wide engagement to support and maintain the physical security of our people, assets and information
- Harmonise people and asset security through proactive and reactive monitoring and response capability
- Maintain a level of preparedness for planned and unplanned security incidents

AWARENESS & TRAINING
- Supporting you to support us
- Implement a structured and innovative approach to security- related training and testing
- Deliver enterprise-wide security-focused training
- Provide guidance to managers and team leaders in security consciousness and assist in delivering key security messages

PROTECTIVE SECURITY PRIORITIES

PREVENT HARM
We will vigorously work toward eliminating physical harm against persons by identifying threats and vulnerabilities and implementing risk reduction strategies.

PROTECT ASSETS
We will be vigilant in preventing loss and damage to our infrastructure as well as identifying fit for purpose security protection processes and systems.

ENSURE COMPLIANCE
We will ensure policies, practices and specialist advice meet the highest ethical and equitable standards, requirements, credentials and legislative compliance.

SUPPORT OPERATIONAL DELIVERY
We will proactively engage with our stakeholders, while providing responsive, professional and relevant advice that enhances critical service delivery to the community.

KEY OUTCOMES

OUTCOME 1
Embed the philosophy of 'Security-in-Depth' providing a multilayer security profile (deter, detect, delay and respond).

OUTCOME 2
Incorporate 'Security-by-Design' across Powerlink's assets/ facilities and supporting planned change management activities to deliver effective security controls.

OUTCOME 3
Deliver an uplift in security awareness, attitudes and behaviours including prompt reporting of security threats or incidents across Powerlink and our stakeholders. stakeholders.

OUTCOME 4
Efficiently utilise resources and leverage technology to achieve security outcomes in alignment with business objectives.

OUTCOME 5
Improve the security maturity when compared to other energy and critical infrastructure asset owners and operators.

SAFE FOR LIFE
Everyone. Everywhere. Everyday.