

Cyber Security Strategy

2020 - 25

January 2019



Part of the Energy Queensland Group

Message from the Head of Cyber Security

I am pleased to share with you the **Cyber Security Strategy 2025** (strategy) for Energy Queensland Limited (Energy Queensland).

This is the first time a cyber security strategy has been developed for Energy Queensland Energex and Ergon Energy Distribution Network Service Providers (DNSP's).

It responds to The Blueprint for the Future Security of the National Electricity Market led by Allan Finkel AO which delivered a plan to maintain security and reliability in the National Electricity Market in light of the significant transition underway, including rapid technological change and the need for increased security.

The strategy covers the Information Communications and Technology (ICT) and Operational Technology (OT) environments supporting our DNSP's and brings together one approach to cyber security. The strategy aims to acknowledge the differences that are inherent in each network and the customers and communities they serve.

This strategy covers the next regulatory period and addresses the challenges associated with an increasingly complex cyber landscape, changes within the global and Australian energy sector and the role we have as one of the largest critical infrastructure energy utilities in Australia.

The EQL cyber security strategy is grounded on four strategic principles:

- Information is an Energy Queensland asset
- Effective information sharing and safeguarding requires a distributed, world's best practice approach that is risk-based
- Public trust through cyber security is critical to Energy Queensland DNSP's
- Cyber security awareness and maturity is integral to Energy Queensland's digital transformation.

In this strategy, we outline key drivers shaping our strategic vision for cyber security to 2025 and a strong plan to achieve that vision.

An Energy Queensland Cyber Security Council has been established to work towards implementing this strategy. As the head of cyber security for Energy Queensland, I look forward to working with you to ensure this strategy's implementation and enduring success.

Peter Price

Head of Corporate Strategy / EGM Strategy Asset Safety and Performance

Document Tracking Details

Network and Non-Network Document Hierarchy Reference Number	Regulatory Proposal Chapter Reference	Document	File Name
NON ICT - 003	7.006	Cyber Security Strategy	EGX ERG 7.006 Cyber Security Strategy JAN19 PUBLIC

Further Information

Further information is available on our websites:

www.energex.com.au

www.ergon.com.au

Contents

Message from the Head of Cyber Security.....	i
1. Introduction.....	1
2. Principles.....	3
3. Drivers shaping our strategy.....	3
4. Our Plan.....	5
4.1 Vision.....	5
4.2 Our Strategic Intent.....	6
5. Strategic Outcomes.....	6
5.1 Outcome 1: Safeguard Information against Cyber Security Threats.....	6
5.2 Outcome 2: Mature and Strengthen Our Cyber Security Posture.....	8
5.3 Outcome 3: Build a Cyber Aware Workforce and Customer Community.....	9
5.4 Outcome 4: Uplift Cyber Security Maturity in Line with Industry.....	11
6. The way forward.....	12

1. Introduction

Cyber security is a constant and dynamic challenge where every day there are thousands of attempts by organised cyber attackers to penetrate Australian businesses, the energy sector, and Energy Queensland.



The energy sector has become a prime target for cyber-attacks and is experiencing a disproportionately large increase when compared with other industries.

Energy infrastructure has become a target of more frequent attacks being launched by nation-states and cyber criminals. As cyber security defenses are ever-improving, attackers have shifted their aim from exploitation to disruption and destruction. Energy Queensland is evolving towards the adoption of integrated and advanced digital technologies to automate and control physical functions to improve performance and adjust to the ever changing energy ecosystem mix. This has created a larger attack surface and new opportunities for malicious cyber threats.

Energy Queensland's cyber security strategy has to be agile and forward leaning to enable us to meet business needs. From a cyber security perspective, we aim to create an environment that prevents, deters, detects and is resilient against cyber-attacks and minimises the vulnerability of our applications, systems and networks.

Security supporting energy reliability

This is the inaugural Energy Queensland cyber security strategy. It represents a shift from security with an emphasis on internal security measures such as:

- protecting the perimeter and patching to keep threats out; and
- sharing knowledge internally.

Towards an emphasis on:

- greater industry, business unit, geographical information sharing and awareness of threats;

- digital transformation to public cloud-based applications;
- greater numbers of users, devices, and uses;
- increase in the amount and diversity of internet connected-devices;
- increasing complexity of technology; and
- interactions with new threat actors and new threat technologies and techniques.

Cyber security aligned with business transformation

The strategy addresses the challenges and key drivers associated with an increasingly complex cyber landscape.

It articulates a compelling vision for the future and a strong plan for realising it by leveraging diverse perspectives, technologies, and experiences across Energy Queensland.

A collaborative approach to implementation will be fostered under a single cyber security strategy and leadership accountability. The overall aim of the strategy is to establish a common understanding and a culture of ownership for cyber security and to align the strategy to the Energy Queensland strategy and business plan as we move forward to 2025.

The strategy is underpinned by four *strategic principles*:

- Cyber security is a fundamental enabler to maintaining public confidence
- Customer and personal information must be protected
- Information is an Energy Queensland asset and the lifeblood of a modern business
- Security needs to continually evolve to keep up to date with threats and business demands.

The four key *strategic outcomes* that we aim to achieve are:

1. ***Safeguard information against cyber security threats***
2. ***Mature and strengthen our cyber security posture***
3. ***Develop a cyber security knowledgeable workforce; and***
4. ***Build our cyber security maturity in line with the industry.***

The success of the strategy hinges on Energy Queensland's ability to establish a governance process, to innovate and to keep a clear line of sight on the way forward as outlined in this document.

2. Principles

There are four strategic principles which form the basis of Energy Queensland's cyber security vision:

Cyber security is a fundamental enabler to maintaining public confidence

We work continuously to protect our ICT and OT systems and information assets from cyber security threats and attacks so that we maintain public confidence in the services we provide to customers and communities across Queensland.

Customer and personal information must be protected

Energy Queensland plays an important role in sharing information publicly information that enables customers and communities to engage with us. At the same time, we have an obligation to protect customer and staff information and the information assets that we have entrusted to us as one of the largest DNSP's in Australia. Compliance with regulatory obligations for information security is fundamental to protecting the sensitive information that we hold.

Information is an Energy Queensland asset and the lifeblood of a modern business

Energy Queensland recognises that information technology is a true enabler of our business plan, we view all information as an asset that must be discoverable and retrievable, consistent with necessary legal obligations and guided by relevant policies, standards, and management frameworks. We manage information assets according to the importance it has to our customers, our staff and to our business.

Security needs to continually evolve to keep up to date with threats and business demands

Energy Queensland security strategy and program must continue to evolve to keep pace with the needs of the business and the changing cyber security threat landscape. Cyber security works in partnership with the business to safeguard and improve our resilience in a sector that is changing rapidly to meet customer, community and market changes.

3. Drivers shaping our strategy

Key drivers shaping Energy Queensland cyber security strategy are below.

<p>New cyber security threat landscape</p> 	<p>The internet is replacing many organisation’s internal networks. Consequently, critical business processes are dependent on external services. This dependence introduces the potential for malicious activities such as denial of service, fraud, interception, and other risks.</p> <p>The energy sector has become a target for malicious cyber security activity.</p>
<p>Increased mobility</p> 	<p>Modern business relies on access from anywhere. To improve business efficiency systems are being delivered directly to the field workforce on mobile devices (phone, tablets, etc.). Having applications and data outside the corporate environment increases the potential attack surface requiring a different approach to security.</p>
<p>Technology adoption</p> 	<p>Security controls must be as close as possible to the information they are protecting. With the adoption of cloud and mobile technologies, the security perimeter must move outwards in order to be effective.</p> <p>Current security measures and technology is unable to evolve to meet the increasing threat landscape. Modern security technology is required to support business digital transformation.</p>
<p>Internet of Things</p> 	<p>The Internet of Things (IoT) brings a unique challenge because of the absence of internationally recognised standards for interoperability, risk management and data security. In addition, interactions between devices in new and novel ways can introduce specific cyber security and other threats, e.g. a fitness tracker leaking troop movements in hostile countries.</p>
<p>Artificial Intelligence</p> 	<p>The use of Artificial Intelligence (AI) technologies to manage the power network introduces risks that the environment may be compromised from an external cyber-attack. Security measures need to be implemented to reduce the likelihood of AI systems being compromise</p>
<p>Critical Infrastructure</p> 	<p>As the owner and operator of critical infrastructure assets and a key stakeholder in state and national resilience arrangements – Energy Queensland is committed to an all-hazards approach to protecting critical infrastructure as specified in the national Critical Infrastructure Resilience Strategy. This includes working with government and other critical infrastructure owners and operators to identify and manage national security risks. As a result of this</p>

	<p>there are particular requirements on how we manage and deliver information systems.</p>
<p>Cyber security risk management</p> 	<p>The ability to protect is progressively compromised. Established methods of information risk management will be eroded or compromised by a variety of threats. Recent history has shown that even small data breaches can result in significant financial and reputational impacts.</p>
<p>Cyber security maturity</p> 	<p>The energy sector is focussed on cyber security maturity now because of the increased threat to the sector. In response to this industry standards have been developed to guide organisations on how to increase their maturity. Energy Queensland is adopting these standards under the direction of the regulator and this will require investment and prioritisation. Timeframes for establishing higher levels of maturity will be subject to business case development.</p>
<p>Technology supply chain vulnerabilities</p> 	<p>Security vulnerabilities within technology offerings are not being disclosed, leaving organisations and individuals open to attack. In addition to this, there is increased concern around technology supply chain which has moved some governments including the Australian Government to restrict a number of technology vendors and service providers.</p>
<p>Global uplift in regulation and compliance</p> 	<p>Governments and regulators are increasingly taking an even greater interest in scrutinising new and existing technology products and services. It is expected this may lead to increased regulation particularly where there are threats of cyber security terrorism.</p>

4. Our Plan

The strategy establishes the vision and mission for Energy Queensland’s Cyber Security Program. These strategies are based on supporting Energy Queensland strategy and business plans encompassing: customer, community, culture, growth and community focus.

4.1 Vision

The vision for cyber security is outlined in the Energy Queensland Business Plan 2018/19:

Achieve global best practice in cyber security

4.2 Our Strategic Intent

Cyber security is an integral and strategic enabler for Energy Queensland's business. Energy Queensland operates a large and complex technology environment this encompasses Information Technology, OT, telecommunications networks, data centres, control rooms, generation and mobile platforms.

It is the role of cyber security to safeguard these systems from attack and maintain the integrity of the data contained within them.

The reliance on data to operate our business is critical to business operations.

Our objectives are to ensure that:

- Energy Queensland's infrastructure and services and systems are resilient to cyber threats
- Our digital and innovation program is empowered through a risk culture
- The community trusts and has confidence in our digital services and this is maintained through measured improvements in cyber security
- The cost and disruption to recover from cyber security incidents is minimised
- Cyber security is managed in a way that meets industry and community expectations.

Our strategic outcomes provide the overall plan for implementing the strategy.

5. Strategic Outcomes

5.1 Outcome 1: Safeguard Information against Cyber Security Threats

We focus security on what is important to Energy Queensland and its customers and communities.

Safeguarding the security of Energy Queensland's information in accordance with its value and its customers' expectations against current and emerging cyber security threats includes:

- Managing security throughout business change
- Addressing security within third parties and supply chains
- Focussing on security governance throughout business and ICT projects and programs
- Application of security in accordance with risk management and compliance obligations, including but not limited to: National privacy principles, General Data Protection Regulation (GDPR), SPAM Act, Telecommunications Act and the Security of Critical Infrastructure Act.

Outcome 1: Safeguard information against cyber security threats

Goals	Activities
1.1 Maintain a register of critical information assets	1.1.1 Identify and record information which must be protected and its location
	1.1.2 Assign ownership of information asset and classify assets
	1.1.3 Manage the information life cycle of each asset
	1.1.4 Ensure that security measures meet protection requirements for each asset classification
1.2 Establish effective governance within Energy Queensland for information risk management	1.2.1 Establish a risk appetite for likely threats against each information asset class
	1.2.2 Establish a framework of information risk governance which integrates with the Energy Queensland risk management framework
1.3 Manage third party information risks	1.3.1 Establish effective commercial controls with all third parties to ensure that all Energy Queensland cyber security requirements are met
	1.3.2 Establish an ongoing program of third-party assurance including but not limited to: <ul style="list-style-type: none"> • Assertion based and certification based compliance • Independent periodic spot checking • Ongoing performance measures and reporting for cyber security • Mandatory breach notification and incident management

	1.3.3	Establish effective on-boarding and off-boarding to meet cyber security requirements	
1.4	Establish processes to address foreseeable information risk events	1.4.1	Conduct threat risk analysis to establish playbooks and processes for managing information security incidents (including but not limited to data leakage)
		1.4.2	Integrate industry and external threat and security intelligence in order to effect timely detection and response to security threats
		1.4.3	Maintain relationships and conduct exercises to ensure an industry-wide capability to respond to sustained cyber-attack against critical infrastructure
1.5	Maintain information risk management across business and ICT system changes	1.5.1	Ensure that changes and enhancements to business processes, information and systems maintain a risk-based approach to our cyber security posture
		1.5.2	Ensure that material risks identified as part of the change management process are owned and managed
		1.5.3	Establish processes and capability to securely share information with external agencies, community groups and customers

5.2 Outcome 2: Mature and Strengthen Our Cyber Security Posture

We adapt and shape security to leverage innovation and address our threats.

Adapting and shaping security posture incorporates technology and security innovation, to ensure that Energy Queensland and its customers and staff can benefit from digital transformation whilst managing evolving threats to information and technology.

Outcome 2: Mature and strengthen our cyber security posture			
Goals	Activities		
2.1	Safely transition to cloud services	2.1.1	Leverage cloud service security to safely transition ICT capability to best of breed and customer-centric services and platforms
		2.1.2	Establish effective governance and visibility around all cloud services
		2.1.3	Ensure the continuity of Energy Queensland ICT services through effective transition in and transition out planning

		2.1.4	Transition security capability to a full 24x7x365 operating model
2.2	Strengthen internal infrastructure and systems to increase resilience	2.2.1	Update the security infrastructure environment to meet the requirements of a modern organisation
		2.2.2	Enhance security infrastructure for services being hosted in a non-cloud environment
		2.2.3	Increase security capability on mobile devices in support of business initiatives making the workforce more mobile
2.3	Enhance cyber security decision making	2.3.1	Enhance logging, monitoring and reporting around cyber security to support timely detection and response for cyber security events
		2.3.2	Obtain and leverage cyber threat intelligence to support adaptation and augmentation of the cyber security control environment
2.4	Adapt and shape security to support new business and technology growth	2.4.1	Develop and implement security architectures that support our changing business technology and landscape
		2.4.2	Develop and implement tactical security measures that support our changing threat landscape
		2.4.3	Develop and implement processes and techniques to effectively prevent, detect, respond and recover from cyber security events
		2.4.4	Develop tools and processes to address cyber security threats upon new platforms such as IOT and mobility

5.3 Outcome 3: Build a Cyber Aware Workforce and Customer Community

We recognise the value of Energy Queensland’s customers, communities and staff having protected information.

In the same way that our industry has undergone a sustained cultural shift toward occupational health and safety, Energy Queensland is embarking upon a cultural shift towards effective and sustainable cyber security.

As cyber security extends beyond Energy Queensland environment this incorporates consideration of our customer community and related cyber security threats.

Outcome 3: Build a cyber aware workforce and customer community

Goals	Activities
3.1 Increase cyber security training, education and awareness	3.1.1 Energy Queensland governance structure will apply consistent performance measurements that enable accountability
	3.1.2 Ensure Energy Queensland leaders demonstrate strong cyber security and risk management leadership qualities and reinforce these through their words and actions
	3.1.3 Ensure continual cyber education for the Energy Queensland workforce
3.2 Strengthen our cyber workforce	3.2.1 Develop and support internal cyber security talent
	3.2.2 Develop internal cyber security mentorship and training
	3.2.3 Demonstrate leading cyber security integrity standards for personnel pre, during and post-employment
	3.2.4 Assign and document owners for all cyber security controls
	3.2.5 Establish security clearance requirements for personal in sensitive and privileged roles for Energy Queensland to meet requirements for a 'fit and proper' person
3.3 Retain cyber talent	3.3.1 Energy Queensland will invest in establishing and maintaining a highly capable cyber workforce by providing advanced training and supporting participation in industry events and knowledge sharing
	3.3.2 Ensure that organisational policies support the attraction and retention of experienced cyber security professionals
3.4 Contribute to the community through cyber security awareness messaging	3.4.1 Provide pro-active education and awareness to customers around relevant cyber security threats and controls
	3.4.2 Respond to and investigate customer cyber security concerns and reports
3.5 Establish enterprise cyber security performance culture	3.5.1 Develop and report key performance indicators for cyber security
	3.5.2 Develop a continuous improvement program to increase performance and reduce risk
	3.5.3 Communication of cyber security performance expectations to all third parties
3.6 Maintain Energy Queensland's reputation as	3.6.1 Contribute to working groups and industry associations to promote cyber security

being a responsible organisation for cyber security

3.6.2 Work with business projects maintain Energy Queensland's reputation by ensuring systems conform to cyber security best practices

5.4 Outcome 4: Uplift Cyber Security Maturity in Line with Industry

Energy Queensland seeks to demonstrate its cyber security maturity in order to meet the expectations of our stakeholders, particularly our customers and the community.

As a result of our digital transformation and the increased threat in the energy sector, Energy Queensland must keep up to date with industry expectations. We will adopt an energy sector specific cyber security maturity framework that will be implemented through to 2025.

Outcome 4: Uplift our cyber security maturity in line with industry

Goals	Activities
4.1 Implement an enterprise-wide cyber security program	4.1.1 Strengthen the governance and leadership to transform Energy Queensland cyber security capabilities
	4.1.2 Evaluate cyber security functions from an efficiency and effectiveness perspective
	4.1.3 Establish and report on end to end visibility of enterprise cyber security controls across the enterprise
4.2 Adopt regulatory guidelines for cyber security maturity capability uplift	4.2.1 Prioritise and improve cybersecurity capabilities using a common set of industry-vetted cyber security practices
	4.2.2 Continually review maturity in accordance with regulatory directives
	4.2.3 Contribute to the development of industry framework to uplift cyber security capability
4.3 Foster partnerships to strengthen Energy Queensland cyber security	4.3.1 Active participation in security forums
	4.3.2 Acquire external perspectives and insights into cyber security by working with vendors and third parties
	4.3.3 Work with industry peers to share information and innovate across industry

6. The way forward

To fulfill our vision to energise Queensland Communities and to achieve global best practice in cyber security we will implement the strategy in the following way.

Regulatory Proposals

Initiatives have been included in the Regulatory Proposals that aligns with the Strategic outcomes in this strategy. These initiatives are paramount for Energy Queensland to achieve the necessary cyber security maturity levels.

Energy Queensland Cyber Security Maturity Roadmap and Action Plan

A roadmap and action plan has been developed to provide direction and the steps to uplift Energy Queensland cyber security maturity.

Energy Queensland Strategy and Business Plans

The strategy will evolve in alignment with Energy Queensland strategy and business planning process.

Energy Queensland ICT Strategy 2030

The strategy will contribute to the ICT strategy 2030 as this is being finalised.

Reviewing our Cyber Security Strategy implementation

In accordance with regulatory requirements, Energy Queensland will periodically review its cyber security maturity strategy, roadmap and action plans.

Energy Queensland will review the performance against the strategy and report on achievement of strategic outcomes and activities. This will ensure that we assess our accomplishments, facilitate good decision-making, hold leaders accountable and demonstrates progress to achievement of Energy Queensland cyber vision.