



Queensland **Cyber Security Strategy** 2025–2027

Trust in government

DELIVERING
FOR QUEENSLAND



Queensland
Government



Copyright

© Department of Customer Services, Open Data and Small and Family Business

This publication is protected by the Copyright Act 1968. This document is licensed by Queensland Government under a Creative Commons Attribution (CC BY 4.0) International licence. In essence, you are free to copy, communicate and adapt this publication, as long as you attribute the work to Queensland Government.



The Queensland Government is committed to providing accessible services to Queenslanders from all cultural and linguistic backgrounds. If you have difficulty in understanding this publication, you can contact us on telephone 13 QGOV (13 74 68) and we will arrange an interpreter to effectively communicate the report to you.

Acknowledgement of Country

The Queensland Government respectfully acknowledges the First Nations peoples in the State of Queensland and the cultural and spiritual connection Aboriginal and Torres Strait Islander people have with the land and sea.

Minister's foreword

The Crisafulli Government is protecting Queenslanders, and their data, by building a resilient, secure and trusted Queensland Government that is able to respond to the evolving cyber threat landscape.

The rapid and expanding digitisation of our society in the 21st century has transformed the lives of Queenslanders, bringing greater choices and opportunities for customers in goods and service delivery. The Queensland Government is no exception, with a range of products and services now accessible online, and we have the ambition to deliver more digital services. That is why we are focusing on delivering secure, effective, efficient and accessible technologies and services.

However, this shift also brings growing digital and information risks. In the cyber domain, state and non-state actors, criminal organisations, issue-motivated groups and individuals, seek to exploit our critical data systems for their own malicious ends. They do this utilising a growing range of rapidly advancing techniques and sophisticated technologies. Cyber attacks, whether on small and family businesses, large institutions of commerce or state entities, have a direct impact on Australia and Queensland's national and economic interests.

As Queensland undergoes greater internationalisation, we must redouble our efforts in forging partnerships with the Australian Government, industry, academia, local governments, small and family businesses and Queenslanders, in order to safeguard our services and information, prepare for and prevent cyber threats and sharpen our focus on our response and recovery capabilities.



The inaugural *Queensland Cyber Security Strategy 2025-2027* demonstrates the Queensland Government's commitment to securing the information Queenslanders have entrusted to us.

This strategy is founded upon three main lines of effort: Strengthening cyber resilience to ensure that government is protected and responsive to cyber threats, enhancing cyber governance and practices to continue enhancing trust in government services, and continuing to address global cyber workforce challenges by developing new ways to attract talented people to protect our critical infrastructure, data and services.

With the increased spotlight on Brisbane, including as the host of the Brisbane 2032 Olympic and Paralympic Games, the Queensland Government recognises the importance of protecting the digital infrastructure supporting major international events, and is part of our ambition to deliver world-class events and experiences for visitors, athletes and Queenslanders alike.

Complementing the *2023-2030 Australian Cyber Security Strategy*, the *Queensland Cyber Security Strategy 2025-2027* empowers the Queensland Government, building a secure, resilient and reliable digital foundation. It marks the Crisafulli Government's commitment to ensuring a more cyber secure Queensland Government.

Steve Minnikin MP

Minister for Customer Services and Open Data
Minister for Small and Family Business

Our Vision

Building a resilient Queensland Government to deliver trusted services for Queenslanders.



Principles

Leverage

We build, use and share to maximise value from common products and services.

Capable

We develop skills and capabilities to enable the public sector to respond and recover effectively from evolving threats.

Collaborate

We work together to prioritise the needs of citizens and strengthen resilience of the public sector.

Empower

We empower the public sector to securely deliver trusted digital services.

Priorities

Resilience

Build and promote ongoing resilience in government service delivery, strengthening our ability to absorb, adapt and respond to the changing threat landscape.

Workforce

Uplift government awareness and strengthen the cyber security workforce through talent development.

Governance

Establish and maintain expectations for governance. Provide clear direction through strategy, policy, culture, metrics and effective assurance.

Objectives

Prioritise the protection of critical government assets and services with targeted investment and initiatives.

Strengthen the public service cyber security workforce through additional training and development.

Enhance the effectiveness of cyber security governance in organisations, project management and procurement.

Expand the delivery of common uplift services to strengthen the cyber security maturity across the sector.

Establish cyber career pathways that guide training investment and talent development.

Grow risk and governance capability, including in our complex supply chains.

Build the cyber threat intelligence function within the sector to further anticipate the evolution of cyber threats.

Enhance insights into cyber workforce strengths and development opportunities.

Provide effective cyber security policies, standards and practical guidance to support and guide the sector.

Enhance incident preparation, response and recovery and coordination for large-scale events.

Provide access to relevant training suited to cyber career development plans.

Increase the quality and breadth of assurance provided to government on its cyber security posture.

Promote supply chain cyber resilience for government.

Develop cyber awareness activities to support capability uplift and build a sustainable security culture.

Collaborate with governments and industry stakeholders to maximise our national cyber readiness.

The *Queensland Cyber Security Strategy 2025–2027*, while acknowledging the differences in its scope and focus areas, complements the *2023–2030 Australian Cyber Security Strategy* (see page 15).

Threat landscape

The digital security environment is rapidly deteriorating, leading to more frequent, larger and more complex cyber security incidents. Threats posed by actors in the cyber domain are increasing.

- One new cybercrime report was made approximately every six minutes.
- More than 84,700 cybercrime reports were made to ReportCyber.
- 28 per cent (or 23,716) of these reports were attributed to Queensland (Queensland reports disproportionately higher rates of cybercrime relative to the population).
- In 2025, the average self-reported cost of cybercrime for small-sized businesses increased to \$56,600 (up 14% from 2024) and \$97,200 for medium businesses (up 55% from 2024).
- Malicious cyber activity poses a significant risk to Queensland networks and systems. Basic attack techniques continue to be effective, identifying the need to collectively uplift cyber maturity. Threat actor groups seek to exploit new technologies such as AI and quantum cryptography as they become more widely available.

The deteriorating cyber domain is spurred further by geopolitical tensions, competition in our region, conflict and global economic conditions. State and non-state actors are seeking to exploit cyber vulnerabilities for profit or other motives. Looking forward, the Australian Security Intelligence Organisation (ASIO) predicts a 'dynamic security environment with an unprecedented number of challenges and a cumulative level of potential harm'.

In 2024, the national terrorism threat level was raised, highlighting the digital environment as a key catalyst for concerning security behaviour in the physical environment. This is because information online spreads quickly and far, with little moderation and vulnerable cohorts who engage with online content.

While threat actor groups have different motivations, their skills are improving, and they are quickly taking advantage of unpatched vulnerabilities or misconfigured systems, gaining entry into restricted systems using advanced phishing and social engineering, or causing disruption through third and fourth parties in the supply chain. Even with strong defences, supply chain cyber incidents are becoming more common and effective.

While the capacity and capability of cybercriminals is increasing, security and intelligence agencies have continued to identify that state-based actors are also exploiting vulnerabilities in many sectors of the economy, further complicating an already complex cybercrime risk environment. Some nation states are growing more willing to target critical infrastructure to further their strategic interests. Recent attribution activity by the Australian Government identifies that nation state threat actors are trying to explore and exploit Australia's important networks, almost certainly mapping systems so they can lay down malware or maintain access in the future.

Operational technology (OT) and Internet of Things (IoT) devices are increasingly targeted by skilled cyber actors more frequently. These devices are used as entry points before attackers pivot to target information technology (IT) systems and data. OT systems often have outdated or unsupported software that can't be patched, making them vulnerable. Since OT is common in critical infrastructure, patching these systems is done carefully to avoid causing disruptions to service delivery. OT and IoT will require additional cyber security focus as Queensland moves into an increasing interconnected and interdependent cyber security future.



Cybercrime impacts in Australia and internationally



47%

of organisations suffered from supply chain cyber attacks in 2024 (*Checkpoint, 2025*)



17,190

phishing scams reported in 2024 (*ScamWatch, 2025*)



200%

increase in supply chain cyber attacks from 2022 to 2023 (*Sonatype, 2023*)



47%

reported their main concern of artificial intelligence being the advancement of adversarial capabilities (*World Economic Forum, 2025*)

48%

of Australian organisations experienced a significant disruption due to cyber attack (*Zscaler, 2025*)



6 mins

the average frequency of cybercrime reports in Australia (*Australian Signals Directorate, 2025*)

Resilience

Build and promote ongoing resilience in government service delivery, strengthening our ability to absorb, adapt and respond to the changing threat landscape.

Queensland communities are resilient to natural disasters. They regularly face natural disasters and significant weather events that disrupt their lives. Similarly, resilience is also required to face the ever-present range of cyber threats facing our state. Our ongoing cyber resilience depends on our ability to anticipate, prepare for, respond and adapt to incremental change, sudden disruptions or shocks in the information and digital environments.

The challenge of complexity and fragility

The systems and information that government depends on to deliver services to Queensland citizens and small and family business are becoming more entwined in our way of life. Current and legacy systems are becoming more complex, and in some cases, more vulnerable. Our infrastructure and systems are increasingly dependent on industry partners. The risk is statewide, but the systems are decentralised and the response is sometimes fragmented. New technologies including artificial intelligence (AI) are creating both opportunities and threats. Understanding and managing these complex, interconnected systems and the information they store and process in this volatile and uncertain environment is a huge task. By supporting cyber security enhanced investments and collaborating across the public sector and our supply chains, we have the best opportunity to overcome these challenges.

A shared responsibility for cyber resilience

Any organisation that provides services for Queenslanders must continue to build their cyber resilience. Governments depend heavily on industry partners to deliver services to citizens and business. Our suppliers in the public, not-for-profit and private sectors all need to play a part in our shared cyber resilience journey; we will succeed by working together.

Leading by example: Queensland Government's role

We will lead by example by developing and sharing cyber resilient behaviour patterns based on international better practice. As the cyber domain changes and we learn better ways to prepare for cyber events, we will update these patterns so they remain current. We will invest in, and build resilient systems and processes and engage with new technologies to reduce and manage risks to acceptable levels. We will promote a culture of cyber security excellence in our people and those we work with, and we will assure our resilience by leveraging data and exercising our systems, processes and infrastructure.

Embedding cyber security into service delivery

We will embed cyber security into the foundations of customer-facing digital services to ensure they are secure, seamless and resilient by design. By enabling trusted digital capabilities, we will support the delivery of consistent, accessible and confidence-inspiring public services. Cyber security will act as a key enabler of innovation and integration, empowering the public sector to transform the customer experience without compromising safety, privacy or trust.

A resilient future for Queensland

Resilience is not just about responding to challenges, it is about thriving in the face of them. By working together, embracing innovation and fostering a culture of excellence, Queensland will continue to lead the way in cyber resilience, ensuring a secure and prosperous future for all.

69%

of large-scale breaches were cyber security incidents (*Australian Signals Directorate, 2024*)

1 in 8

reported cybercrimes in Australia affect state or local government (*Queensland Audit Office, 2024*)

28%

of cybercrimes reported in Australia happen in Queensland, the highest of an Australian state or territory. However, Queensland does not have the highest average monetary loss (*Australian Signals Directorate, 2025*)



How we'll get there

To deliver on our objectives,
the Queensland Government will:

Prepare and exercise incident management and response plans and embed cyber security fundamentals like threat intelligence, training and collaboration into the way we do business.

Expand and target the delivery of common cyber uplift services, advice, policy and guidance.

Leverage the Cyber Security Fund to address critical cyber security risks.

Support cyber enhanced digital and IT system investments under the \$1 billion Queensland Government Digital Fund by promoting 'secure by design' principles.

Create economies of scale and increase collaboration by making cyber security products and services available to Queensland Government including local government.

Adopt new technologies such as AI and new approaches like 'zero trust' to strengthen preparedness, defences and cyber teams' capability.

Educate small and family business on cyber threats and recovery strategies and connect them with resources, programs and support such as Cyber Wardens.

Develop cyber resilience across system lifecycles and supply chains by uplifting cyber risk management and improving procurement guidance and tools to deliver sustainable, secure and resilient operations.

Maximise use of common cyber procurement panels and standing offer arrangements to promote common solutions, enable targeted engagement with pre-qualified suppliers and simplify purchasing for state and local government.

Support local cyber businesses by connecting suppliers and government to enhance government supply chains, maximise workforce opportunities and strengthen local capability.

2024

Top 5 scam types by loss

(combined data)



Investment

**\$945.0
million**



Payment redirection

**\$152.6
million**



Romance

**\$156.8
million**



Phishing

**\$84.5
million**



Remote access

**\$106.0
million**

The losses for the Top 5 scam types accounted for 71% of total losses in 2024 in Australia

**\$4.28
million**

the average cost of a data
breach for an organisation in
Australia (*IBM, 2024*)



\$56,600

the average self-reported cost of
cybercrime for small businesses
(*Australian Signals Directorate, 2025*)

Workforce

Uplift government awareness and strengthen the cyber security workforce through talent development.



Meeting the demand for cyber talent

To safeguard government, we must ensure the right people and processes are in place to mitigate risks to respond quickly to cyber attacks and maximise the security of new technologies as they emerge.

Taking a strategic approach to the cyber workforce

To tackle these challenges, the *Queensland Government Cyber Workforce Strategic Plan 2025–2027* focuses on building a cyber resilient workforce through three strategic priorities:

- Retrain and retain: attract and retain valued talent.
- Enhance capacity: understanding cyber skills supply and demand and enabling effective matching to opportunities for growth of the cyber talent pipeline.
- Nurture capability: develop solutions to scale and enhance cyber security skills and learning across the Queensland Government.

Building our cyber culture

Core to Queensland Government's resilience is embedding cyber skills universally, recognising the imperative to have capability at all levels of the sector, ultimately creating and building a supportive cyber culture for Queensland.

Fostering a culture of cyber security awareness and supporting capability uplift helps create an environment where everyone is empowered to protect themselves, the Queensland Government and its customers from cyber security threats. This, in turn, enables the protection of Queensland Government services and information.

Queensland case study

Increasing supply

To ensure the Queensland Government has an effective cyber workforce in an environment of rising demand for cyber security professionals, we have partnered with TAFE Queensland over the past six years to support 148 public sector employees graduate with a Certificate IV in Cyber Security. The program has attracted a wide range of IT and frontline staff from Cairns to Toowoomba and has achieved a 25 per cent conversion to cyber jobs in the sector. The current 2024–25 cohort has 56 participants keen to graduate and protect Queenslanders.

Supporting executives to manage cyber threats

Active executive leadership is vital for protecting public sector information, citizen data and service continuity. To support this, we have partnered with the Australian Institute of Company Directors (AICD) to offer interactive sessions tailored for Queensland Government senior executives focusing on cyber risks and their role in enhancing cyber capability. These sessions help clarify responsibilities, provide practical guidance on cyber governance and include a cyber crisis case study. Since 2021, 310 Queensland Government executives have participated in these programs, enhancing their understanding of the evolving cyber threat landscape and uplifting their cyber skills.

How we'll get there

To deliver on our objectives, the Queensland Government will:

Working with industry and academia, provide actionable, practical advice to entities and leadership to support informed decision-making and protection against cyber threats.

Enable agencies to assess the current cyber workforce to identify skills gaps and implement practices to meet evolving needs.

Provide direction to tackle workforce challenges, create impactful opportunities and prioritise workforce diversity in order to bring new perspectives, capabilities and talent to bolster new and innovative approaches.

Implement the *Cyber Workforce Strategic Plan 2025–2027* to address emerging cyber workforce changes, focusing on training, attracting and retaining diverse talent.

Utilise the Queensland Government cyber skills framework to build awareness of the skills, knowledge and attributes required in the cyber workforce.

Support workforce development and maximise access to training for maintaining and enhancing cyber capabilities including through TAFE Queensland to provide cyber qualifications for public servants.

Explore training opportunities (including for early career and professional talent) to address specific needs, strengthen public sector cyber security capability through reskilling, and retention programs to grow and retain cyber talent.

Expand the reach and tailor cyber security awareness materials to highlight emerging scams and threats to public servants.

In Australia

30,000

more cyber security workers are needed to fill employment gaps within the next 4 years (*CyberCX, 2022*)

74%

of survey respondents state they are facing significant cyber security skills gaps (*AustCyber, 2023*)

21%

of the cyber security workforce is female (*CyberCX, 2022*)

15%

of cyber security talent in Australia is in Queensland, the third highest of any state or territory (*CyberCX, 2021*)

Governance

Set high expectations for governance.
Provide clear direction through strategy, policy,
culture, metrics and effective assurance.

With the rapidly evolving cyber threat landscape, effective governance is not just important, but imperative to our security efforts. The Queensland public sector must ensure strong policies, effective risk management and governance frameworks which focus on establishing the capability to protect organisations from cyber threats. More effective cyber governance supports building and maintaining citizens' trust in government.

Effective governance is the backbone of cyber resilience in the Queensland Government. A culture that embraces good governance ensures policies, processes and priorities are effectively aligned to safeguard the state's digital assets and services and underpins our ability to prevent, respond to and recover from cyber incidents. It provides a structured approach to decision-making, risk management and resource allocation—all crucial in the face of evolving cyber threats.

Cyber security's role in enterprise governance

The Queensland public sector must endeavour to adapt to the changing environment and integrate cyber security in all systems and practices. Integration through broader strategic planning processes and governance structures would further enhance and maximise opportunities to bring cyber security to the forefront of maintaining public trust, maximising resilience of services that protect citizens' privacy. This approach helps to maximise the alignment of cyber security objectives to government's priorities, protecting citizens' privacy, maintaining public trust and maximising the resilience of services.

Effective governance ensures resources are distributed efficiently and strategically. It enables decision-makers to allocate funding and expertise to the areas of highest risk or greatest impact, ensuring that cyber security investments deliver maximum value.

The pursuit of effective cyber risk management

Strong governance is underpinned by intelligence-led data-driven decisions informed by effective risk management systems. Effective systems of cyber security governance provide structure to allow executives to prioritise threats based on targeting preferences, security vulnerabilities, potential impacts on government services and critical infrastructure.

The emerging cyber threat landscape brings new challenges to systems of governance that require government to be agile and adapt to the evolving security environment. Conducting strategic cyber threat analysis, examining critical impacts to government services through cyber disruption and assessing capacity to protect systems from sophisticated cyber attacks is now part of the enterprise risk management function in public sector organisations.

Consistency in this renewal of enterprise risk systems will help ensure cyber risks are addressed comprehensively and financial efficiencies and economies of scale can be leveraged.

Instilling confidence

Good governance frameworks are underpinned by data and performance metrics. These metrics help measure the effectiveness of resource allocation, ensuring investments align with organisational needs and provide ongoing value. Data provides the critical evidence needed to provide assurance to Queenslanders that not only are our organisations compliant with recognised security policies and standards, but that our systems—and their data—are actually secure.

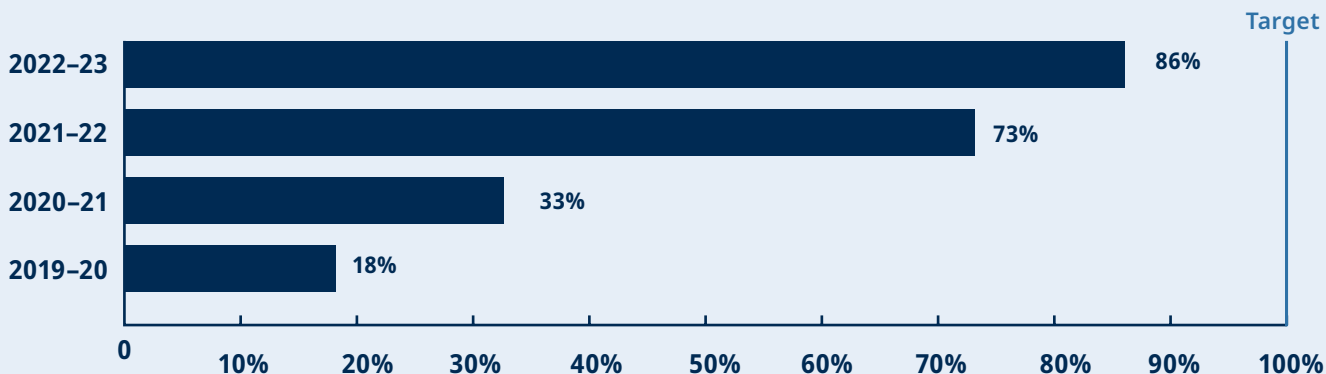
Queenslanders rely on digital infrastructure and assets to deliver services that are vital for everyday life and place their trust in the Queensland Government to securely manage these services and their information.



68%

growth in the number of government organisations with operational information security management systems.
(Queensland Audit Office, 2024)

Percentage of departments with operational information security management systems



Source: Queensland Audit Office from Department of Transport and Main Roads—Cyber Security Unit ISMS report.

How we'll get there

To deliver on our objectives, the Queensland Government will:

Increase governance effectiveness and support continuous improvement in governance bodies by providing boards and executives with strategic threat intelligence, increased visibility of cyber risk and data insights.

Engage governance leads in communities of practice to share lessons, collaborate and build a shared knowledge repository within the public service.

Foster collaboration across government and industry sectors to enhance governance capability and drive innovation through new products and services and enhancing cyber procurement.

Strengthen cyber security assurance by expanding information and cyber security policy and governance requirements to a broader range of government entities in accordance with the information and cyber security policy (IS18) and other regulatory requirements, including the *Security of Critical Infrastructure Act 2018*.

Strengthen risk management capabilities to enhance resilience through common services, tools, risk management (including in supply chains) advice and guidance.

Provide actionable resources and threat intelligence to support evidence-based decision-making and effective policy implementation.

Continue to partner with the Australian Government on strategy, policy and frameworks, including through the National Cyber Steering Committee and Data and Digital Ministers, and amplify their impact.

Collaborate with other jurisdictions and industry to coordinate strategy and share timely, actionable threat intelligence.

Align and integrate Queensland's information and cyber security policies with state and national protective security arrangements.

Leverage data from annual IS18 return and other sources (e.g. Essential Eight dashboard pilot) to improve assessment, investment decisions, assurance and benchmarking processes.

Queensland Government

cyber security governance framework

Strong cyber security governance is essential to safeguard the Queensland Government's systems, data and services. As cyber threats become more frequent and sophisticated, clear roles, responsibilities and oversight is vital.

This framework provides a summary of the Queensland Government's current cyber security governance. The cyber security landscape spans across digital, disaster management and security/counter-terrorism governance arrangements including intersection with Australian Government strategies and plans.

Queensland Cabinet and relevant committees

- Approves Queensland whole-of-government cyber security strategy.
- Oversees funding via budget and digital investment prioritisation.
- Queensland Security Cabinet Committee and Queensland Disaster Management Committee.

Cyber Security Unit, Department of Customer Services, Open Data and Small and Family Business

- Leads whole-of-government cyber security strategy, governance, policy and investment.
- Supports and uplifts agency capability through tools, training, communities of practice and expert guidance.
- Coordinates whole-of-government responses to incidents and provides shared services to reduce risk.

Queensland Government agencies

- Own and manage agency cyber security risks and implement policy and controls.
- Respond to incidents and collaborate with the Cyber Security Unit on prevention/preparedness/response/recovery as required
- Participate in relevant whole-of-government committees, working groups and communities of practice.

Australian Government

- Sets Australian Government cyber security strategy and policy.
- Works with states and territories to strengthen national cyber resilience.
- Cooperation on responses to national cyber incidents through the Cyber Incident Management Arrangements and Australian Cyber Response Plan.

Why is the governance framework important?

Broader government:

establishes clear direction, accountability and oversight to align cyber efforts across government.

For agencies:

provides policy (IS18), tools and expert support to manage cyber risks and guidance and decision-making for incident management with confidence and clarity.

Queensland citizens:

strengthens trust through transparent, secure and well-governed cyber security controls and services.

Queensland case study

Preventing incidents through a coordinated response

In November 2023, Australian governments began tracking multiple critical vulnerabilities in widely used software products worldwide. These vulnerabilities could be used for unauthorised access to those systems. Over 150 potentially vulnerable systems were detected in Australia (including 20 in Queensland).


The Queensland Government escalated a response under the Queensland Government Cyber Security Hazard Plan. This ensured coordinated whole-of-government monitoring, analysis and engagement to help prevent and protect against any malicious cyber activity occurring to Queensland.

A Queensland Government cyber security incident response team worked with national partners to monitor, analyse and respond to the evolving situation. Threat alerts containing technical advice were circulated broadly, government entities were also provided specific guidance for risk mitigation and remediation. The team also engaged directly with potentially exposed government entities. Through these efforts, the Department of Customer Services, Open Data and Small and Family Business remediated all instances of Queensland Government entity exposure and removed the risk of exploit.

As a result, the Queensland Government was able to remedy vulnerability exposure that could have resulted in an incident that could cause significant loss of services or sensitive information to Queenslanders.

Australian Government cyber strategy

The *Queensland Cyber Security Strategy 2025–2027* complements the Australian Government’s roadmap through its ‘horizons’, and the focus areas known as ‘shields’ of the *2023–2030 Australian Cyber Security Strategy*. The actions under the priority areas of the *Queensland Cyber Security Strategy 2025–2027* aim to support the Australian Government’s strategic aspirations to be a world leader in cyber security by 2030. Queensland will continue to contribute to and monitor the Australian cyber security strategy’s future horizons.

	Resilience	Workforce	Governance
Shield 1 Strong businesses and citizens			
Shield 2 Safe technology			
Shield 3 World-class threat sharing and blocking			
Shield 4 Protected critical infrastructure			
Shield 5 Sovereign capabilities			
Shield 6 Resilient region and global leadership			

DELIVERING
FOR QUEENSLAND



Queensland
Government