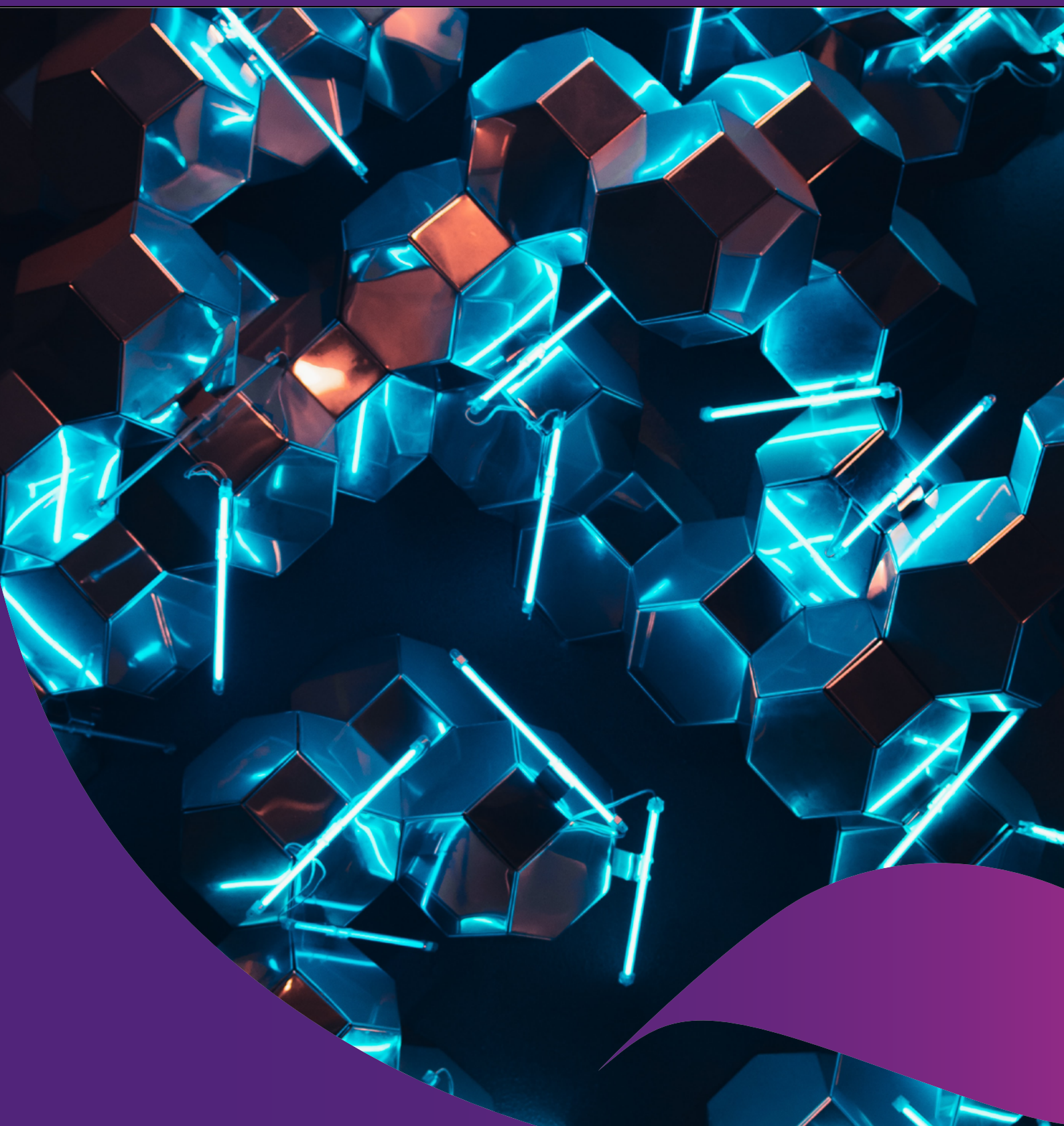




THE UNIVERSITY
OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

Cyber Security Strategy 2021 – 2023



Context

UQ's Cyber Security Strategy directly supports the [Enterprise IT Strategy](#) and [UQ's strategic plan](#), and defines UQ's approach to managing cyber security over the next three years (2021 – 2023). This strategy was developed to align with the [Australian Cyber Security Strategy](#) and UQ's cyber security risk appetite statement, which is defined according to [UQ's Enterprise Risk Management Framework](#).

UQ is strongly committed to enhancing and effectively managing cyber security, and this strategy considers the constantly evolving cyber security threat landscape and the diverse needs of the University. In particular, there are several key factors which have influenced our strategic direction:

COVID-19 and resource constraints: COVID-19 has profoundly impacted the higher education sector, and has created a number of challenges that impact cyber security. The increase in remote working and teaching has heightened UQ's cyber security risk, while travel restrictions have impacted UQ's international student and research markets, creating financial constraints that limit IT's resources. In the next three years IT will continue to prioritise cyber security by taking an economically sustainable, risk-based approach.

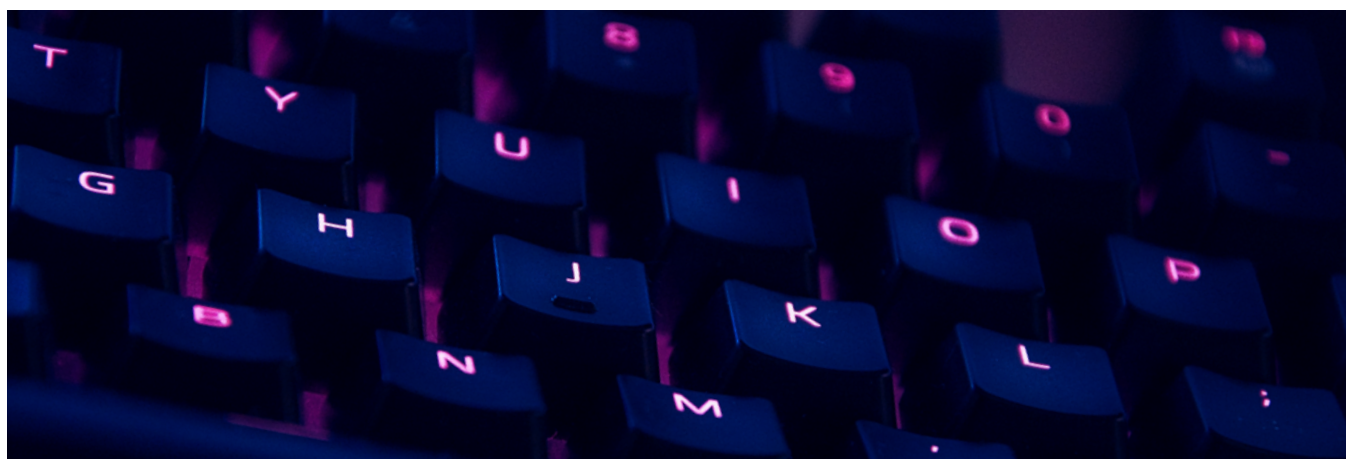
Countering foreign interference: UQ engages significantly with the international community through teaching, research collaborations and industry or government partnerships. This open environment of international collaboration provides significant benefits, but also increases the risk of foreign interference. Governments are beginning to consider universities as critical infrastructure, and while this increases opportunities for government research partnerships, it makes it more important than ever to protect our information assets. The Australian Government has already launched the [Defence Industry Security Program](#) (DISP) which sets standards to protect defence research undertaken by universities, and we can expect other industries (e.g. agriculture, medicine) to adopt this approach. In the next three years, UQ

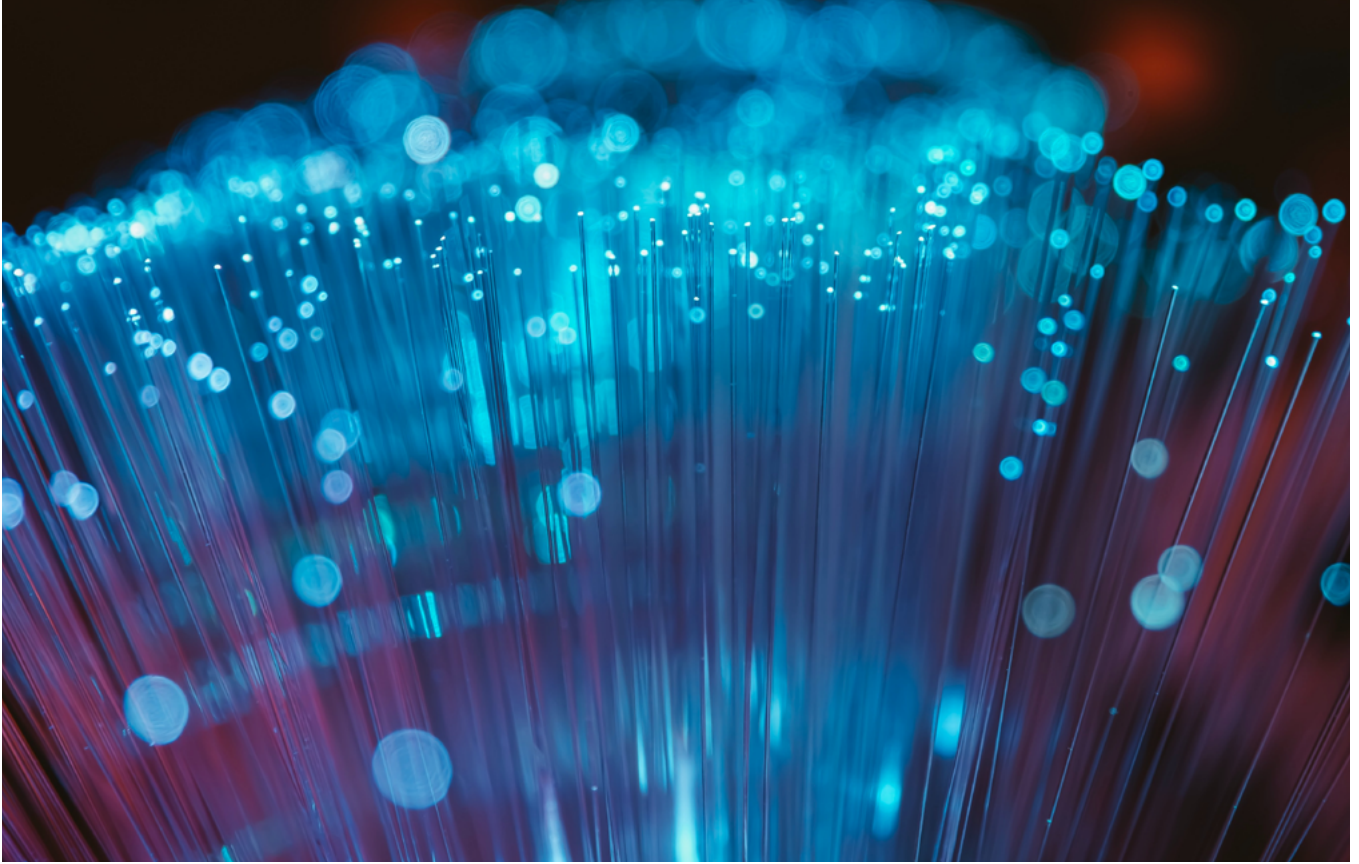
will also commit to initiatives in response to the University Foreign Interference Taskforce's (UFIT) [Guidelines to Counter Foreign Interference in the Australian University Sector](#).

An evolving threat landscape: The cyber security threat environment is aggressive, well organised and constantly changing. We all have a role to play when it comes to cyber security – attackers are increasingly circumventing technical controls and targeting account holders (e.g. staff and students) who inadvertently 'open the door' to attackers. These attackers seek to harm UQ's reputation, steal intellectual property, commit financial fraud, and undermine the integrity of student grades and research. Ransomware attacks involving data exfiltration (where criminals demand a ransom to regain access to files or prevent a data breach) are a major threat and pose a significant risk to the UQ community. It is imperative that UQ continues to respond to changing threats in an agile manner by managing a plethora of risks concurrently and prioritising effectively.

Maintaining a premium digital experience: UQ's information technology environment is vast and constantly changing to meet the needs of research, teaching, learning and professional services. The Enterprise IT Strategy defines the need for a premium digital experience via valuable, flexible and easy-to-use services, while also ensuring that UQ's security needs are met.

We are not alone: Cyber security criminals share information and work together to attack people and organisations, supported by a thriving black market economy of cybercrime products and services. Fortunately, there is a growing ecosystem of people and organisations working collaboratively to counter this threat, including UQ's own [AusCERT](#) and the [Australasian Higher Education Cybersecurity Service](#) (AHECS). Governments are also playing a greater role facilitating collaborations and intelligence and knowledge sharing to increase the cyber security capabilities of organisations such as UQ.





Our goal

To reduce and manage UQ's cyber security risks to enable effective research, teaching and community engagement.

Our principles

- **Cyber security is everyone's responsibility:** Promote collective and individual responsibility to create and maintain a mature cyber-safe culture.
- **Cyber security is an enabler:** Deliver trustworthy services based on demonstrably sound security technologies and practices.
- **Defence in depth:** Adopt a layered mix of physical, technical and administrative controls to detect, prevent, mitigate and recover from cyber threats.
- **Balanced security management:** Implement security controls that balance risk mitigation against cost and the UQ community's digital experience to maximise benefits for the University.
- **Manage complexity:** Ensure that cyber security controls and solutions integrate and work in concert with underlying information systems and processes to reduce risk and minimise complexity wherever possible.
- **Secure by design:** Provide leadership, governance and oversight to ensure cyber security requirements are met during the design, development, selection and management of information systems.
- **Continuous adaptation:** Review and improve information security management in response to security incidents and keep pace with changes to the University, information technology, security technology and the threat landscape.
- **Engage and collaborate:** Build and engage in mutually beneficial partnerships throughout the cyber and higher education industries to enhance protection against common threats.
- **Automate first:** Utilise automated processes where feasible to enable consistent, accurate and timely deployment of security controls with reduced dependence on manual labour.



Key objectives

1. Adopt a risk-based approach to cyber security that supports and enables UQ's operations and objectives while mitigating cyber security risks and protecting the privacy of our UQ community.

- Proactively identify, prioritise and manage cyber security risks to reduce UQ's overall risk level.
- Provide IT services that enable business processes without compromising security.
- Where possible, adopt security solutions that protect UQ without detracting from the digital experience.
- Adopt security solutions that enable mobility and the use of cloud-based IT services.
- Implement controls and mechanisms to mitigate the risk of personal information breaches and streamline the management of personal information.

2. Protect UQ's data and systems through effective technical controls and secure IT services.

- Adopt integrated security solutions that work in concert to deliver advanced security capabilities with reduced operational overheads.
- Increase automation of security capabilities (such as incident detection and response) to enhance protection and reduce operational costs.
- Incorporate cyber security into the architectural design of all new IT and information systems or processes, regardless of whether they are operated internally or by a third party.
- Align UQ's key cyber security controls with best practice frameworks such as the Australian Signals Directorate's (ASD) [Essential Eight](#), and emerge as an exemplar within the higher education sector.

3. Protect UQ's data and systems through effective governance and information management.

- Review and update procedures and standards within the [Cyber Security Framework](#) when required to adapt to new risks, technologies and business requirements.
- Where possible, align UQ's cyber security management with industry-recognised frameworks and standards to provide assurance to stakeholders and increase opportunities for industry partnerships.
- Provide training, resources and support as required to improve compliance with internal and relevant external cyber security policies, procedures and standards.
- Protect the confidentiality, integrity and availability of UQ's information and intellectual property by identifying and classifying information assets, enhancing the Information Asset Register, and implementing consistent and appropriate information management controls.

4. Build a security-oriented culture, where members of the UQ community are engaged and aware of the role they play in protecting UQ's data and information.

- Clearly define cyber security roles, responsibilities and authorities across UQ to ensure that cyber risks are owned and managed by the correct individuals or groups. Encourage all staff to identify and report cyber security risks.
- Expand the Data and Cyber Security Awareness Campaign to encourage behavioural change in stakeholders who either hold a critical role within the University, or are commonly targeted by cyber security criminals.
- Frame cyber security challenges and solutions through the lens of the diverse UQ community.
- Provide timely and relevant cyber security information to the UQ community to protect them from cyber threats and bullying, both at work and in their personal life.
- Promote cyber security as an enabler and safeguard of academic freedom and free intellectual inquiry.
- Build cyber security awareness and competencies into staff and student outcomes.





5. Collaborate widely to gain knowledge and strengthen the security capability both at UQ and within the higher education sector.

- Align UQ's cyber security approach with UFIT's [Guidelines to Counter Foreign Interference in the Higher Education Sector](#), and emerge as an exemplar within the higher education sector.
- Leverage the [Australasian Higher Education Cybersecurity Service](#) (AHECS) as a mechanism to share knowledge, collaborate in sector-wide projects and provide a common voice from the sector in discussions relating to cyber security.
- Share information with industry and cyber defence peers to reduce the sector's risk profile without compromising UQ's security position.
- Participate in cyber security initiatives coordinated by [Universities Australia](#) and the [Group of Eight](#).
- Continue to build relationships with the [Australian Cyber Security Centre](#) (ACSC), industry peers and information security service providers to strengthen cyber and information security capabilities within UQ and across the sector.
- Benchmark UQ's cyber security maturity and capabilities against other Australian universities to foster continuous improvement.
- Actively contribute to and generate value from communities of practice, including [CAUDIT](#) and [QUDIT](#).
- Build relationships within UQ's academic community to leverage subject matter expertise and improve support to mature internal cyber security capabilities.
- Leverage AusCERT's information security capabilities to provide exceptional operational security to UQ.

Success measures

We will measure UQ's approach to cyber security management against our peers via industry benchmarks, and aim to place within the **top quartile of our sector**.

Achieving our strategic objectives will help UQ improve its cyber security maturity. We aim to increase UQ's maturity rating across several domains, which each link to one or more of our objectives.

In each domain, we aim to increase UQ's maturity rating to a **level 4**, or '**measured**' level of maturity, where processes are defined, measured for effectiveness, monitored, regularly reviewed or audited, and partially automated. More information on the maturity rating scale can be found below.

Domain	Key objectives
Security operations and incident response	1, 4 and 5
Disaster recovery and business continuity	1, 2 and 5
Legal compliance (e.g. Information Privacy Act 2009)	1, 3 and 4
Asset management (e.g. workstations, software, servers)	1, 2 and 3
Third party management (e.g. vendor and supplier management)	1 and 2
Access control (e.g. passwords, account provisioning)	1, 2, 3 and 4
Risk management	1 - 5
Information management (e.g. data governance and controls)	3 and 4
Software development and acquisition	1 and 2

Target maturity ratings are based on UQ's ability to develop and implement cyber security frameworks, initiatives and controls.

Maturity rating	Definition
1	Initial: Processes are typically undocumented or loosely defined and in a state of dynamic change.
2	Developing: Processes are generally evolving and partially documented. This is a developing environment for emerging but inconsistent processes.
3	Defined: Processes have defined and documented standards, roles and responsibilities. These standard processes are used to establish consistency.
4	Measured: Processes are measured to work effectively, monitored, regularly reviewed or audited and partially automated.
5	Optimised: Processes are proactive and characterised by a focus on continuous process improvement and optimisation, best practice, risk mitigation and automated workflows.



Contact

Office of the CIO

The University of Queensland
Level 4, Prentice Building, St Lucia
Brisbane QLD 4072

T +61 (07) 3346 6881

E cio@uq.edu.au

W its.uq.edu.au