University of Southern Queensland

CYBER SECURITY STRATEGY 2021–2025

WHO WE ARE

VISION

The University of Southern Queensland will be renowned for our innovation and excellence in education, student experience, research and engagement.

STRATEGIC IMPERATIVES

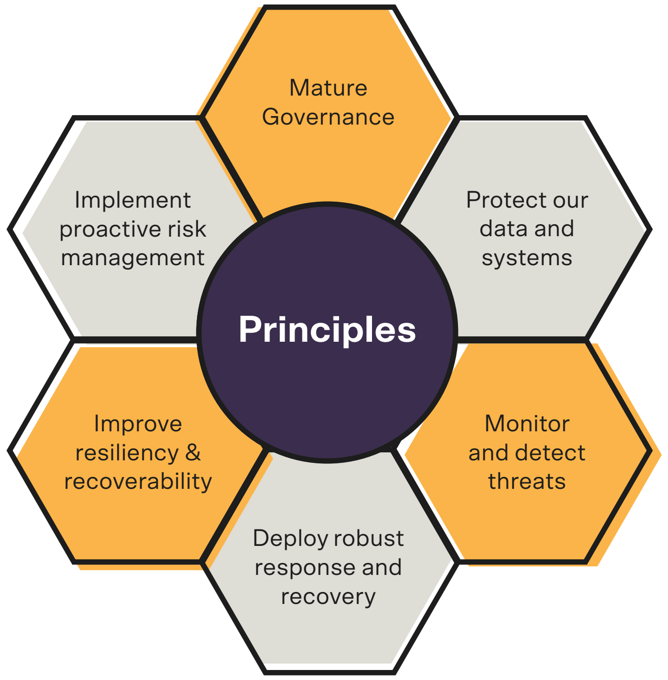
STRATEGIC GROWTH | DIFFERENTIATION | INNOVATION | SUSTAINABILITY

OUR STRATEGIC APPROACH

MISSION

To support UniSQ's objectives by securely enabling its initiatives and operations while protecting it from threats to the availability, integrity and confidentiality of systems and data.

We will benchmark against the ASD/ACSC Strategies to Mitigate Cyber Security Incidents, and extend and adapt to meet the specific needs and challenges of the Higher Education sector.


Mature Governance
Implement proactive risk management
Protect our data and systems
Principles
Improve resiliency & recoverability
Monitor and detect threats
Deploy robust response and recovery

OBJECTIVES

- Align with enterprise risk tolerance and expectations
- Understand, learn from and respond to our environment
- Implement effective measures to protect against known threats
- Have resilience systems and processes against unforeseen threats
- Detect threats that were not able to be protected against
- Rapidly respond to events and incidents
- Recover to normal operations as soon as feasible and possible

GOVERN | PROTECT | DETECT | RESPOND & RECOVER

RISK LANDSCAPE

IF WE DON'T MANAGE THESE RISKS WE HAVE A PROBLEM

Disruption to Service

External threat actors (criminals, nation states, activists) seek to deny access to (DoS), disrupt, deface and inappropriately access and use our systems and resources.

If we don't protect our systems from external malicious disruption or influence, critical business process will be negatively impacted effecting the student experience, our ability to produce research and engage with our communities.

Reputational Risk

Cyber incidents can be **highly visible in the media and broadly reported** and discussed.

If we fail to broadly address cyber threats and account for reputational considerations, we may lose market standing, suffer impact due to perceived negativity about our brand, and degradation of our partnerships.

Loss of Data

Data is valuable and desirable for cyber criminals, nation states and malicious individuals to attain (theft) or deny access to (ransomware). Threats can be external actors, external actors who have managed to gain internal access, or internal. As a custodian of data (including sensitive research), its loss can not only affect UniSQ, but also those we hold data on behalf of.

If we don't protect our data, we run the risk of reduced user confidence, negative media coverage, negative external compliance scrutiny and impacted business processes.

Financial Impact

Key business process are increasingly **digitalised and critical** to 'normal' business operation.

If we don't pay attention to cyber fraud, financially motivated threats, or business interruption motivated attacks, UniSQ faces a potential financial impact, impacting our sustainability and growth imperative.

Third Party Risk

We **partner with and consume services** from external organisations. They have risks which we must be aware of and manage to mitigate impact upon UniSQ.

If we don't effectively manage our external partners, we risk failing to meet our aspirations and expectations due to failings in our supply chain and our partners.

Regulatory and Compliance

Government, regulators, funding bodies and partners have expectations and requirements. Expectations for protection against foreign interference is increasing and is forecast to continue to increase.

If we fail to maintain compliance, we will be subject to negative public and regulator perception, and increased cost of compliance going forward.

University of Southern Queensland

CYBER SECURITY STRATEGY 2021–2025

GOVERN	PROTECT	DETECT	RESPOND & RECOVER
• Monitor overall risk exposure • Prioritise activity based on evidence • Monitor for effectiveness	• Block known threats • Build resilience in staff and systems	• Detect threats we can't block	• Rapidly respond to events & incidents • Safely return to known good state • Based on data, continuously improve

HOW WE WILL CONNECT ACTIVITY TO STRATEGY

• Maintain & Review Strategy • Consult with Stakeholders • Oversight Major Initiatives • Monitor Key Risks & Metrics • Resource appropriately	• Secure network perimeter • Harden endpoints • Mitigate phishing • Control Identity & Access • Build Awareness & Education	• Seek external threat intelligence • Monitor for anomalies • Monitor systems, endpoints and access • Data loss prevention	• Automate response and recovery where possible • Analyse incidents • Communicate • Practice Recovery

MAJOR CYBER SECURITY INITIATIVES

• Cyber Security Strategy • Benchmarking against ASD essential 8 & Higher Education sector • Counter foreign interference framework • Higher Education sector threat intelligence sharing	• Revitalised Awareness & Education Program • Phishing Simulation • Expansion of Endpoint and Identity controls • Multi-Factor Authentication (MFA)	• Expand event capture & machine learning analysis • Internal threat detection platform	• Security Orchestration & Automated Response platform • Major Cyber Security Exercise

HOW WE WILL REPORT

• Benchmarking results against ASD essential 8 & Higher Education sector • Control improvement initiatives • Internal strategy aligned metrics (network, endpoint, phishing)	• Perimeter network blocking activity • Phishing attempts blocked • Phishing simulation results	• Endpoint malware detections • Account compromise	• Incidents causing significant business impact