

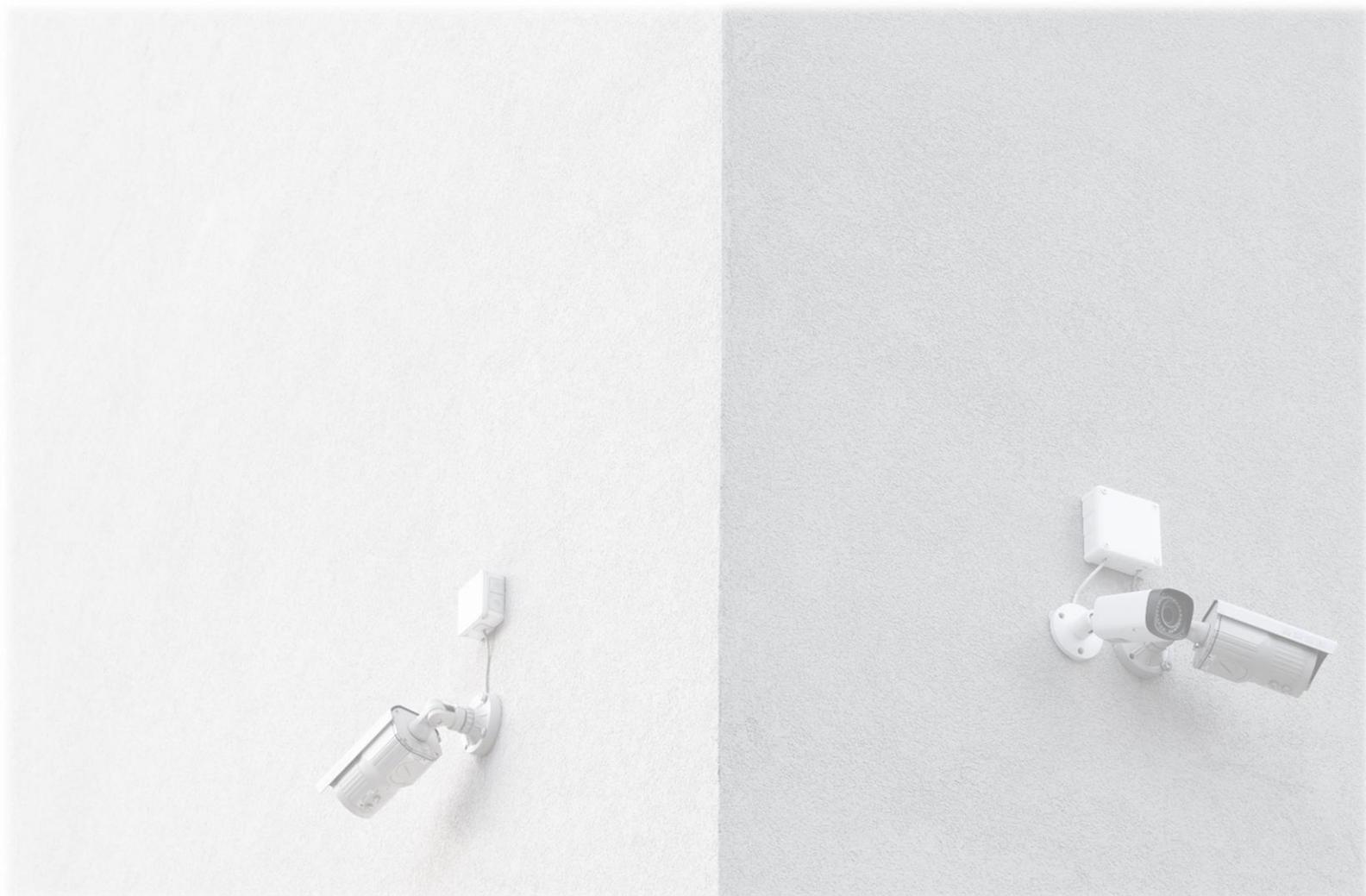
**Queanbeyan-Palerang Regional Council (QPRC)**

# **Cyber Security Strategy**



## Revision History

Version	Date	Author	Description
0.1	12 <sup>th</sup> Jul 2021	Doug Stapleton and Shane Zwajgenberg	Initial Draft
0.2	26 <sup>th</sup> Jul 2021	Doug Stapleton and Shane Zwajgenberg	Revised Draft
0.3	16 <sup>th</sup> Sep 2021	Shane Zwajgenberg	Revised Draft ver.2
1.0	18 <sup>th</sup> Sep 2021	Peter John	Final review and revision



# Table of Contents

---

Stakeholder Engagement ..... 4

Executive Summary ..... 5

Cyber security Steering Committee ..... 9

Response to Cyber security Incidents ..... 10

ICT Strategic Plan ..... 11

Citizen-centric Services ..... 11

Cyber Workforce ..... 12

Staff Planning ..... 12

NSW Digital Cyber Security Strategy ..... 12

Security Compliance ..... 12

Essential Eight Compliance ..... 13

QPRC Network Diagram ..... 15

Emerging Areas for Consideration ..... 16

Addendum - Implementation roadmap

# Stakeholder Engagement

---

## Context:

The Architecture Practice (TAP) developed the QPRC's draft Cyber Security Strategy in consultation with the Digital Team who manages the ICT operations for QPRC.

## Interviews:

Initial stakeholder interviews were conducted at QPRC, Queanbeyan NSW, on 17<sup>th</sup> June 2021 with QPRC's Digital Team members.

## QPRC Attendees:

Name	Title	Email Address
Peter John	Service Manager Digital	Sensitive content; redacted
Matt Dale	Program Coordinator Network	Sensitive content; redacted
Bevan-Leigh Hussey	Systems Officer	Sensitive content; redacted
Chris Walters	Senior Solutions Architect	Sensitive content; redacted

## TAP Attendees:

Name	Title	Email Address
Doug Stapleton	Senior Security Architect	Sensitive content; redacted
Shane Zwajgenberg	Business Consultant	Sensitive content; redacted

# Executive Summary

---

The ICT landscape is constantly evolving with new threats and malicious code, and sophisticated malware being developed every day. Effective cyber security controls consist of technical measures and staff training to ensure that they understand the threat environment and are not compromising the technical controls. The actions of malicious actors in cyberspace have become one of the top risks organisations face globally. This Cyber Security Strategy will inform the steps that QPRC needs to take and focus on over the next three years (2021 -2024) to increase the organisational security maturity and create a safe, secure, and resilient council.

This strategy consists of four main themes:

**Governance**: To increase cyber governance through the implementation of a Cyber Security Steering Committee. This committee would focus on current and emerging cyber security issues. The Steering Committee would meet quarterly and provide an opportunity for the Executives to focus on the cyber risks to QPRC operations and progress towards increasing cyber maturity.

**Trust of Citizens**: A successfully implemented digital interaction with QPRC should enhance community trust and confidence in the

Council's digital services and the new 'digital by default' approach to service provision.

**Security Expertise**: Increasing cybers maturity will ultimately require increased investment in specialist IT security staff or consultants. Several models could support increasing this much-needed capability for QPRC.

**Security Compliance**: While the Australian Cyber Security Centre's (ACSC) Essential Eight mitigations are not mandatory for QPRC and other councils, there is a shift towards this. These mitigations may become a legislative requirement in time. QPRC has made good progress on this alignment, and 'Security Compliance' is a core accomplishment and pillar of QPRC's Cyber Strategy.

To turn our community's long term aspirations and strategic priorities into reality, QPRC has built itself on five strategic pillars of Community, Choice, Character, Connection and Capability. Ensuring that security is a foundational component of all business changes will assist with building trust with all of those who interact with QPRC. Over the next three years, QPRC would like to focus on being the best for the internal staff and the community it supports.

# Roles and Responsibilities in Cyber

The Australian Government's Security Strategy has been illustrated in the figure below as a baseline for how industry, Government and the community should work together to create a safer and more inclusive security ecosystem. The Australian Government's vision is for a more secure online world for all Australians, their businesses, and the essential services we all depend on. Below is an example of the security responsibilities and security ecosystem that the Australian Government sees as appropriate. This security strategy helps align QPRC with the strategic objectives of the Australian Government.

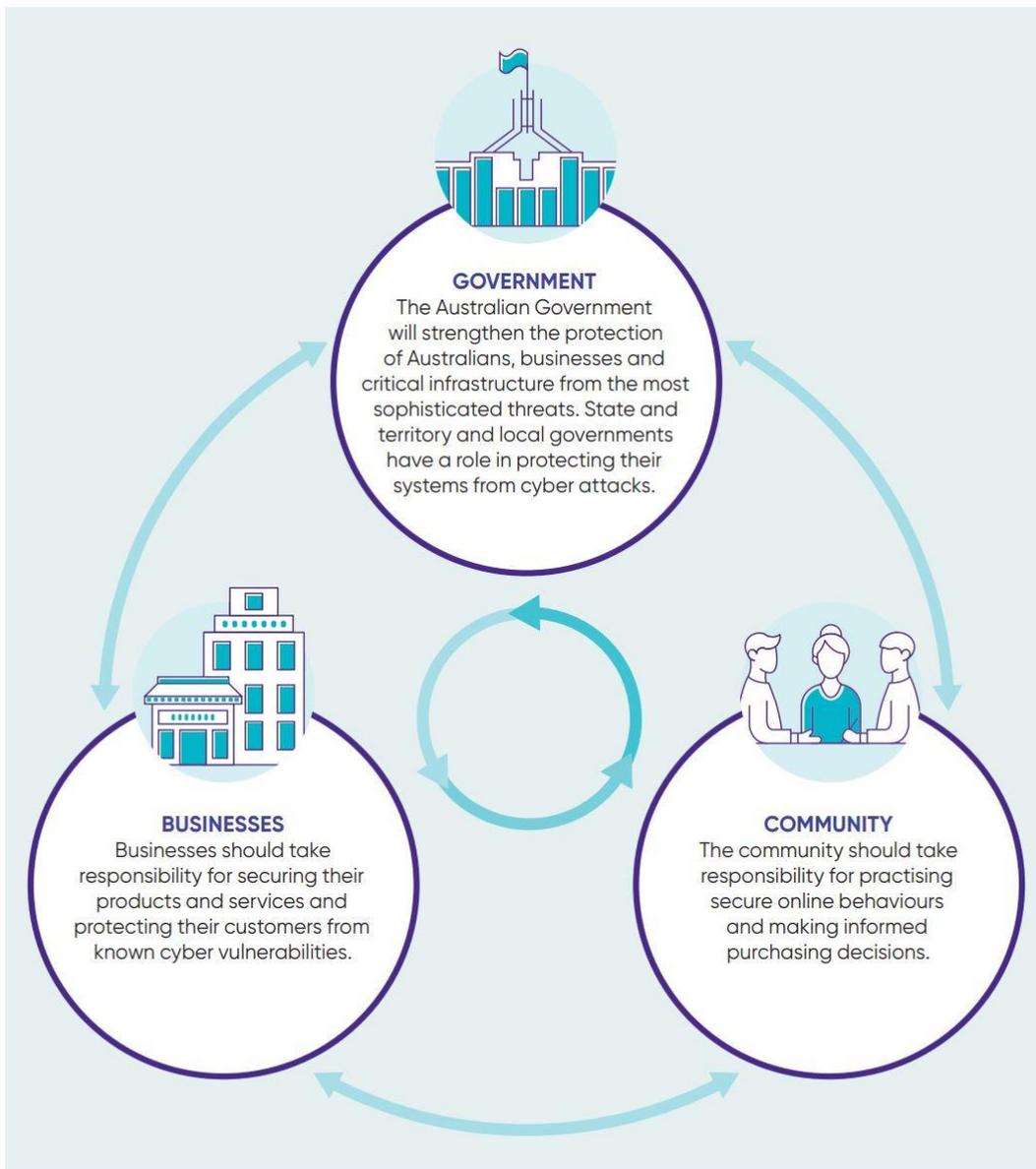
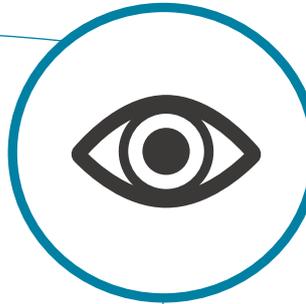


Figure 1 - Roles and Responsibilities in cyber security, Australian Cyber Security Strategy 2020

# Approach to Security 2021 - 2024



## *Vision*

Deliver effective and efficient security for QPRC and the members of the community to minimise the risk of cyber-attacks.



## *Mission*

Leverage innovative solutions to create and sustain trusted systems.



## *Pillars*

- Governance
- Trust of Citizens
- Cyber Workforce
- Security Compliance



## *Focus Areas*

- Security Maturity
- Security Workforce Planning
- Compliance
- Emerging areas for consideration

# Security Awareness Maturity

To realize QPRC's desired security vision, the current focus is on uplifting the cyber maturity across QPRC and better planning for the future. QPRC's current operating state has some well-known challenges that have been identified through various business reviews and stakeholder engagement. Below is a visual representation of the security awareness maturity model that will guide the future uplift of its maturity across the organisation.

## SECURITY AWARENESS MATURITY MODEL™

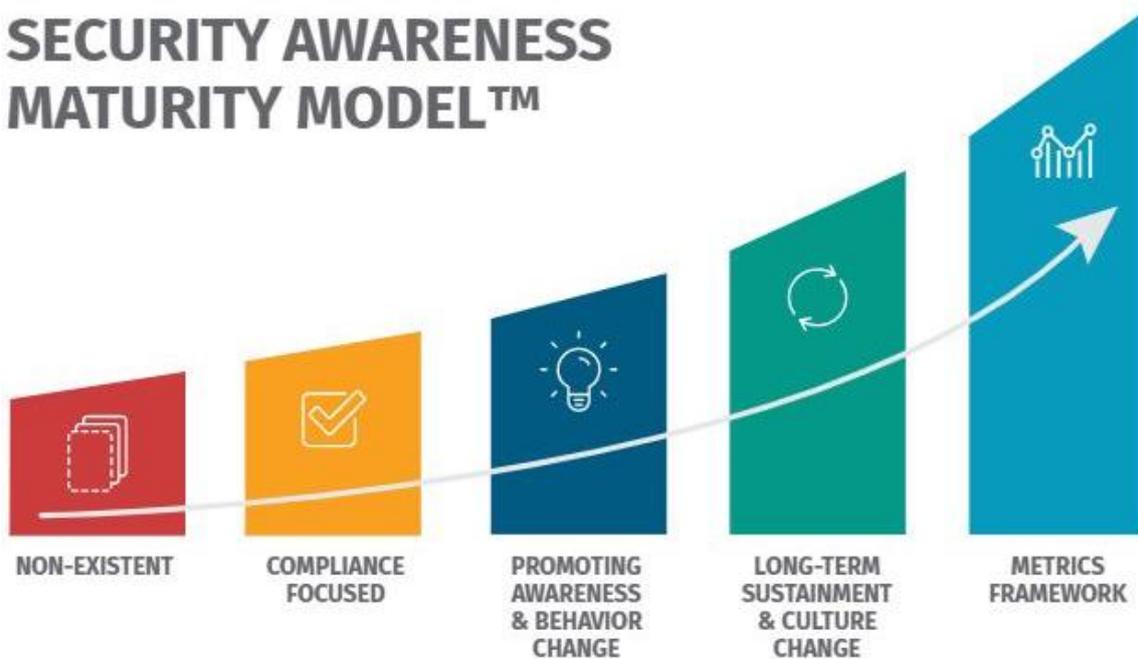


Figure 2 - SANS Security Awareness maturity model

# Governance

Cyber security is becoming a vastly more vital function within society in today's world. The rise of ransomware has become an existential threat to business function and has decreased the communities trust in corporations. A public list of disclosed ransomware demands is available at the following website <https://ransomwhe.re>. This list currently reporting USD \$61million<sup>1</sup> in ransomware demands but notes that a reported total ransomware revenue in 2020 was up to \$350 million.

Funding cyber security is not intuitively obvious; the more that is spent to become

'secure', typically the less visible the results are. Good security is invisible in that sense and can lead to complacency as people feel like it has been a long time since an incident occurred. This is in stark contrast with other public infrastructure investments, where the more that is spent, the more visible the results are.

Governance in a cyber security context can be further divided into the role and make-up of the governance committee and, secondly, an incident response plan to ensure that there is an effective and coordinated organisational response to a cyber incident.

## Cyber Security Steering Committee

When considering the formation of QPRC's Cyber Security Steering Committee (CSSC), it is important to note that this does not replace existing operational and tactical committees such as the Business Continuity Plan run by the DR team and the Crisis Management Team (CMT). The steering committee will focus quarterly on funding and the ongoing conversation. It provides an opportunity for the Executives to be informed and focus on cyber security initiatives, business impact and budget and funding issues.

A key recommendation of this report is that QPRC forms a Cyber Security Committee. This will align and help implement the 'Risk Management' principle from the 'Governance Lighthouse'<sup>2</sup> as part of QPRC's *Good Governance Framework*. It also demonstrates the leading by example principle within the *NSW Digital Cyber Security Strategy*<sup>4</sup>.

The Steering Committee typically would meet quarterly and includes those with a managerial or senior leadership role.

The membership consists of the following stakeholders:



<sup>1</sup> As at 14 July 2021

<sup>2</sup> An internally focussed best practice model of good governance which is advocated by the NSW Audit Office.

The CSC will provide oversight and provide leadership in the following:

- Advise the Executive and the Audit Risk Improvement Committee (ARIC) on the current cyber risk exposure and mitigations that are in place.
- Review QPRC's cyber security breach response and crisis management plan.
- Review the Council's most valuable assets and sensitive information (critical assets or 'crown jewels') to ensure that adequate controls are in place to protect them.
- Review QPRC's ability to identify and manage new and emerging cyber threats.
- Assess the adequacy of resources and funding for cyber security activities.

## Response to cyber security Incidents

A Cyber Security Incident Response Plan needs to be developed specifically for QPRC and will cover:

- Identification of what constitutes a cyber security incident.
- Who is notified?
- What are the immediate actions (shutting down servers, etc.)?
- Are there standard response scenarios pre-authorized by the Cyber Security Committee or another group such as the Crisis Management Team?

QPRC will develop a Cyber Security Incident Response Plan in the specific context of QPRC operations, complementing the existing plans, including the ICT Disaster Recovery (DR) plan.



# Trust of Citizens

A successfully implemented digital interaction with QPRC should enhance the community's trust and confidence in the Council's digital services and the new 'digital by default' approach to service design and provision.

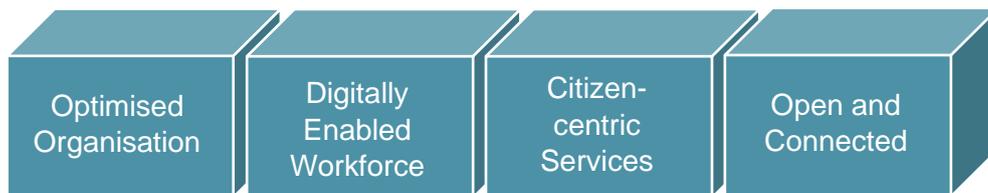
Citizens in the community have several concerns about moving to a 'digital by default' method of interacting with the Council. There are many recent reports of scammers defrauding citizens, and it has become hard to work out how to trust those we interact with digitally. Those concerns can be summarised as follows:

As noted below, a successfully implemented digital interaction with citizens would align well with the third key strategy, 'Citizen-centric Services', and its related objectives from QPRC's ICT Strategic Plan.

QPRC will enhance citizen trust in its digital services to improve the uptake of the 'digital by default' approach to Council service provision.

## ICT Strategic Plan

Four key strategies underpin this plan:



## Citizen-centric Services<sup>3</sup>

Citizen-centric services cover the areas of People, Process and Technology in the three related objectives:

- Objective 3.1 Co-design and Collaboration (promote the voice of the community in ICT products and services through co-design and collaboration).
- Objective 3.2 Communication (engage the community and collect their input and insights regularly, through services such as livestream and your voice).
- Objective 3.3 Digitally Enabled Services, Smart Cities and IoT (utilise digitally-enabled services, Smart City initiatives and the 'Internet of Things (IoT) to meet community expectations).

---

<sup>3</sup> QPRC ICT Strategy 2020-2024

# Cyber Workforce

---

## Staff Planning

Given the increasing focus organisations in public and private sectors have on managing their cyber security, The demand for experienced ICT security staff is highly competitive. The consequence of this is that experienced cyber security professionals can be expensive and difficult to recruit. To date, QPRC has met this need by predominantly contracting out cyber security guidance to specialised firms. Increasing QPRC's internal

capability in cyber security skills and resources would require dedicated funding. This discussion is fundamental to the types of the ongoing conversation about risk and exposure that would be managed by the Cyber Security Steering Committee referenced above. Building this capability strongly aligns with the first and second principles noted below of the *NSW Digital Cyber Security Strategy*.

## NSW Digital Cyber Security Strategy<sup>4</sup>

The NSW Digital Cyber Security Strategy concentrates on four principles for execution:

- Lead by example in best practice and cyber resilience.
- Be progressive and proactive to allow the cyber workforce to expand.
- Seek opportunities to grow cyber industry commercialisation.
- Provide practical support to reduce barriers to business growth.

# Security Compliance

---

One of the focus areas of QPRC's ICT strategy is to protect the privacy of data entrusted to it under the Australian Privacy Principles<sup>5</sup>. As part of that focus, confidence in the identity of QPRC's ICT systems users, be they employees or contractors, will be enhanced over time by implementing an Identity and Access Management (IAM) solution. IAM is a framework of policies and technologies ensuring that only the right users have the appropriate access to QPRC's technology resources.

---

<sup>4</sup> <https://www.digital.nsw.gov.au/transformation/cyber-security/cyber-security-strategy>

<sup>5</sup> <https://www.oaic.gov.au/privacy/australian-privacy-principles/>

## Essential Eight Compliance

Whilst the Australian Cyber Security Centre's Essential Eight<sup>6</sup> is currently optional on a 'best efforts' basis, it is becoming essential over time, with a legislative compliance requirement being foreshadowed. QPRC has made good progress on this alignment, and under the 'Security Compliance,' it is a significant accomplishment and will continue to be a pillar of this Cyber Security Strategy. The latest report of QPRC's Essential Eight compliance generated on 17<sup>th</sup> June 2021 is as follows:

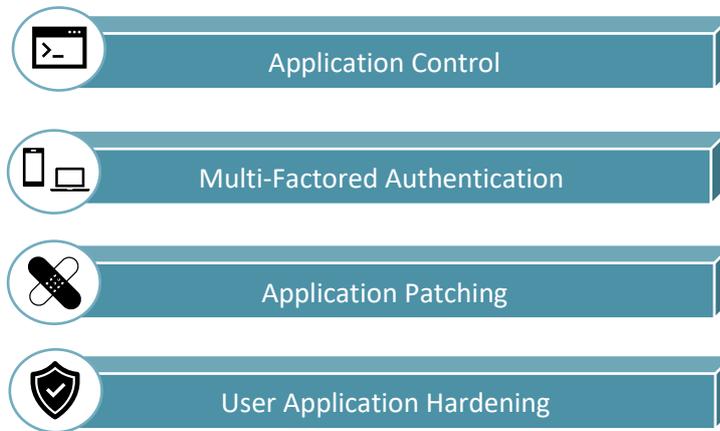
**Sensitive content; redacted**

---

<sup>6</sup> <https://www.cyber.gov.au/acsc/view-all-content/essential-eight>

## Compliance Uplift

QPRC is working towards achieving a higher level of compliance against the Essential Eight, with the ongoing projects that are focused on the areas of:



This progress was documented in detail in the 2021 QPRC cyber security baseline review.

QPRC will continue to focus on Security Compliance to ensure alignment with ASCS's Essential Eight ahead of it becoming a legislative compliance requirement.



## QPRC Network Diagram

QPRC has recently mapped their current state network layout. This visual clearly maps the current state and gives a consumable overview of QPRC's network.

Sensitive content; redacted

Sensitive content; redacted

### QPRC Cyber Security Overview – 26 May 2021

#### Legend



# Emerging Areas for Consideration

Several areas will be under consideration in the Cyber Security Strategy for the next three years. These will seek to understand better the operational technology security and the provision of technology in critical services such as the water and sewage plants and other areas.

Another emerging area would be the increasing engagement with 'Smart Cities' in the analysis of service design and provision. As this evolves, QPRC will benefit by further understanding the benefits this can add. Finally, the isolation of the Supervisory Control and Data Acquisition (SCADA) systems from the internet may be critical to maintaining their integrity.

Security will forever be an evolving component of every Organisation. QPRC aims to become a secure and protected Organisation that is informed and understand security from all perspectives.



## PRIVACY

Be wary of what is shared and with whom



## PASSWORDS

Create strong passwords to be secure



## SUSPICIOUS MESSAGING

Treat any unexpected messages with caution



## SURFING SAFELY

Avoid malware—keep to trusted websites



## ONLINE FINANCE AND PAYMENTS

Keep financial details from prying eyes



## TABLETS AND MOBILES

Be mindful when using free Wi-Fi



## BACKUPS AND PROTECTION

Backup and update for safety



## REPORTING

Keep everyone safe by reporting scams

# IMPLEMENTATION ROAD MAP

This Implementation Roadmap provides an indicative plan to meet the strategies and key objectives contained within the cyber security strategy. It is positioned as 'indicative', given that the owner of each accountable area needs to continually review and refine the underlying approach to ensure that the objectives and outcomes are achieved, rather than following a pre-defined, activity-based plan.

ID	Objective	Outcomes	What needs to be done? [2021 – 2024]	Time-frame	Owner
1	<ul style="list-style-type: none"> <li>• <b>Implementation of a Cyber Security Steering Committee</b></li> </ul>	<ul style="list-style-type: none"> <li>• focus on current and emerging cyber security issues</li> <li>• focus on cyber security initiatives, business impact and budget and funding issues.</li> <li>• Active and visible leadership by the Executive</li> <li>• Ensure adequate controls are in place to protect QPRC's critical assets or 'crown jewels'.</li> </ul>	<ul style="list-style-type: none"> <li>• meet quarterly</li> <li>• report to the Executive and ARIC as required</li> <li>• develop and classify Council's most valuable ICT assets and sensitive information systems</li> </ul>	2022 onwards	Service Manager, Digital
2	<ul style="list-style-type: none"> <li>• <b>Incident response plan</b></li> </ul>	<ul style="list-style-type: none"> <li>• an effective and coordinated organisational response to a cyber incident.</li> </ul>	<ul style="list-style-type: none"> <li>• develop a standards-based cyber Incident response plan, endorsed by the Executive</li> </ul>	December 2022	Service Manager, Digital

ID	Objective	Outcomes	What needs to be done? [2021 – 2024]	Time-frame	Owner
3	<ul style="list-style-type: none"> <li>• ASD 'Essential Eight' framework implementation</li> </ul>	<ul style="list-style-type: none"> <li>• enhance the community's trust and confidence in the Council's digital services</li> <li>• mitigate any potential reputational damage</li> <li>• Improve the Confidentiality, Integrity and Availability (CIA) of QPRC's network and systems</li> </ul>	<ul style="list-style-type: none"> <li>• continue Digital's work towards achieving a higher Maturity Level (ML 2 or 3) for all Essential Eight controls</li> </ul>	2021-24	Service Manager, Digital
4	<ul style="list-style-type: none"> <li>• Uplifting the cyber maturity across QPRC</li> </ul>	<ul style="list-style-type: none"> <li>• promote cyber awareness and behaviour change</li> <li>• long-term sustainment and cyber culture change</li> <li>• achieve a phish-prone score (KRI) of &lt; 4% for the organisation</li> </ul>	<ul style="list-style-type: none"> <li>• quarterly cyber awareness campaigns for all staff and councillors</li> <li>• quarterly phishing simulation tests for all staff and councillors</li> <li>• yearly Security Culture Survey (SCS)</li> <li>• yearly Security Awareness Proficiency Assessment (SAPA)</li> </ul>	2022 onwards	Service Manager, Digital

# Notes

---

---

---

---

---

---

---

---

---

---

