Cyber Security Strategy

2019-2022

V1.0

Queensland Government Vision

"A secure and resilient government for a safe and prosperous Queensland."

CLASSIFICATION: OFFICIAL

Contents

REVISION HISTORY

Ver	Notes	Author	Date of Change
1.0	Final document	ECQ Director of Technology	30/1/2019

ECQ Strategic Objectives

Our Purpose: Supporting democratic electoral process by preparing for, conducting and reporting on elections in Queensland.

Our Vision: To be an **EVOLVING** Commission, **TRUSTED** and **RESPECTED** by the community.

Relevant Electoral Commission of Queensland (ECQ) Strategic Objectives and Key Performance Indicators:

- Conduct boundary reviews with transparency, integrity and accountability.
- Electoral roll is accurate.
- Election delivery in a transparent and accountable manner.
- Results delivered in an accurate and timely manner.
- Integrity training for all ECQ's staff.
- Improved governance mechanisms to plan for and deliver elections.

Cyber Security Strategy Objectives

The ECQ is focussing on building simplified, standardised and, most importantly, secure platforms for the future. This is because, despite the threats outlined in this document, the ECQ must and will take advantage of technology that assists with delivering secure products and services if it increases its effectiveness and efficiency.

Drawing on its history of delivering trusted electoral services, the ECQ will ensure end-to-end verifiable elections (E2EVE) whilst introducing technology to replace, complement or enhance electoral systems and process. This is to ensure that ECQ's key stakeholders - Queensland electors – can have confidence both in electoral systems and processes, and in election results.

The ECQ will adopt the Queensland Government Information Security principles and policies IS18:2018 (ISO 27001) in a sustainable way, ensuring that the benefits expected from that strategy are delivered.

Queensland Government Cyber Security Principles

1. Cyber security is a CEO and leadership responsibility.
2. Cyber security risk management and governance are to be embedded in agency management processes.
3. Transparency of an agency's cyber risk and remediation is essential to ongoing improvement.
4. Cyber security threat and incident information is proactively shared between Queensland government agencies to help strengthen our government-wide defences.

Cyber Security in an ECQ context

Worldwide attention on electoral processes and cyber security is higher than ever. There are ongoing reports of attempts by foreign agents to influence public sentiment about electoral participants and processes and/or to interfere in electoral system integrity. The ECQ has other responsibilities beyond election day, including: boundary and electoral arrangement management, administering and enforcing funding and disclosure schemes, and political party registration and regulation. Most public concern however, is regarding elections and electoral processes.

This is why in December 2018 the Council of Australian Governments (COAG) – the peak intergovernmental forum in Australia – issued a strongly worded communique[i] highlighting the threat to Australian sovereignty from acts of foreign interference, acts which are increasingly

[i] https://www.coag.gov.au/sites/default/files/communique/coag-communique-dec-2018.pdf

enabled by technological developments. As that communique outlines, inter-jurisdictional collaboration between electoral management bodies and security and government agencies will intensify in the coming years to identify and combat these cyber threats.

The remainder of this strategy outlines the ECQ's pillars of cyber security, the challenges that the ECQ currently faces, the principles that will drive the ECQ's actions, and a high-level action plan. The following graphic explains the relationship between these different elements of the strategy:

ECQ Pillars of Cyber Security

There are five pillars of cyber security within the ECQ. All principles and actions outlined and undertaken by the ECQ in this and other documents (e.g. the action plan) are aligned with one or more of these pillars.

- **Integrity**: Protection of electoral information, systems, and services from unauthorised modification or destruction. Integrity is considered in an end-to-end manner, from the consumers of the information to the technology platforms providing the service.
- **Confidentiality**: Protection of information from unauthorised disclosure to unauthorised individuals, systems, or entities. Confidentiality is data oriented.
- **Availability**: Timely, reliable access to data and information services by authorised users. Availability is service oriented.
- **Non-repudiation**: The ability to correlate, with high certainty, a recorded action with its originating individual or entity. Non-repudiation is entity oriented.
- **Authentication**: The ability to verify the identity of an individual or entity. Authentication is entity oriented.

The Key Challenges Influencing ECQ Cyber Security

The ECQ is responsible for the cyber security of its stakeholders' data. This includes the integrity of election results, the Queensland electoral management system, the Queensland electoral roll and a variety of data sets with varying confidentiality requirements. Nineteen challenges have been identified which affect how the ECQ manages these responsibilities. In summary, these challenges can be categorised as relating to either the ECQ's organisational maturity or its technical capacity and capability.

Guiding Principles to address the Challenges

There are 13 guiding principles underpinning this strategy. These are drawn from a suite of principles relevant to cyber security, but highlighting those of most direct relevance to the ECQ.

Accountable Officer Responsibility. Formal cyber security responsibility, advocacy, and ownership is held or nominated by the agency chief executive. Cyber security priorities are driven by the business owners.

Alignment with Whole-of-Government Requirements. Information assets will be aligned to the Queensland Government and organisational enterprise architectures, information security policy and the Queensland Government information security classification requirements, and appropriately managed to their sensitivity and criticality.

Trusted Security. Best practise cyber security will be utilised to protect the information provided to the ECQ by the community and will be designed and implemented where possible to promote a trusted relationship.

Integrous Delivery. The integrity of the ECQ's service delivery and information assets will be maintained and kept at the highest possible level. Integrity will be maintained and complimented through the addition of security controls while ensuring the transparency of service delivery is not impacted.

Risk Focused Evolution. The need to maintain and manage cyber security and associated business risks will be considered when implementing and procuring new IT systems. Considerations of accuracy, integrity, and transparency should not be majorly compromised during any product implementation or procurement process.

Sustainable Cyber Security. Sourcing and procurement of cyber security products and vendors should be completed with consideration of their institutional stature[ii] with all aspects of contracts assessed and considered. The procurement of cyber security solutions will be considered on a whole-of-life cost and benefit basis.

Adequate Response. The ECQ's cyber security incident response activities will be appropriate and resourced effectively to better enable security teams to mitigate associated risks; response activities will be prioritised with the public's security in mind.

Design and Implement for Resiliency and Integrity. All cyber security architecture should be designed and implemented to enable change with a minimum of effort, to survive failure, and based on the assumption that at some point part or all the systems will be compromised.

Focus on Seamless Experience. The way people experience Security, whether end-users, or internal or external customers (all stakeholders), must be a central consideration. Wherever possible stakeholders should not even know controls are present because they have been so well designed and seamlessly implemented. Stakeholders should be able to quickly and easily achieve their business outcomes without onerous cyber security controls.

Effective Recovery. Security recovery activities will be focused on restoring functionality while ensuring the security of the information owned or managed by the ECQ. Recovery from system failure (through malfunction or other) will undergo continued iteration with lessons gleaned from previous incidents feeding future activities.

Education and Awareness. Cyber security will be a consistently practised and a regular aspect of the workplace culture. The ECQ will maintain a high level of security awareness amongst all personnel

---

[ii] *Institutional Stature is a combined definition of reputation, standing, pedigree, principles, values, etc.*

by emphasising that everyone has responsibility and accountability for the protection of information assets.

Proactive detection capabilities. The ability to effectively detect and pre-emptively mitigate potential vulnerabilities and risks in the ECQ environment is invaluable in modern cyber security practice. The ECQ will develop and maintain the capabilities to effectively detect and monitor potential cyber security events, where possible detective capabilities should be included in any system.

Reduce threat of Cyber Incidents. Also known as 'defence in depth' there is no single control that can remove the risk of cyber security incidents; it is for this reason a framework should be implemented to produce a myriad of compensating controls. The ECQ will develop and implement a range of effective control sets to mitigate the threat of cyber incident.

Turning strategy into action

The ECQ's cyber security policy will contain specific guidance and practises to effectively manage business and technology practises. Refer to the cyber security policy for specific details.

The ECQ's cyber security strategy will be a reference document for ECQ's governance committees, teams and groups to manage, monitor and prioritise the implementation of cyber security priorities, projects and principles.

The ECQ will work with both new and trusted partners to improve its services and the cyber security of those services.

All existing and future ECQ priorities, projects and programs will align with the cyber security strategy pillars and principles.

Review triggers and timelines

This strategy and its associated policy and activities will be **immediately reviewed** if:

- The ECQ's risk appetite articulated in its Risk Management Framework changes substantially as agreed by the Electoral Commissioner as advised by the Senior Management Team; and
- Specific incidents occur or substantial triggers arise which are not currently captured in the identified challenges in this strategy, or are not part of an existing recommendation as outlined in the action plan.

Otherwise, this strategy is to be reviewed concurrent with the ECQ's Strategic Plan to ensure alignment between the ECQ's strategic objectives, high-level strategies, and key performance indicators.