# Cyber Security Strategy
## 2021-2024

*Mitigating a significant business risk – cyber security is not "just an IT thing"*

*Taking a truly coordinated and collaborative approach to sharing resources and establishing practices to increase cyber maturity and resilience across the Local Government sector.*

| Common Gaps[1] | Strategic Priorities | Initiatives | Potential LGITSA Partners | Existing Capabilities & Resources |
|---|---|---|---|---|
| **Security Governance**<br>Strategy<br>Policies & procedures<br>Cyber awareness<br>Third parties<br>Risk management<br>Audits<br><br>**System Security**<br>Passwords<br>Privileged accounts<br>User access<br>Vulnerability management<br><br>**Change Management**<br>Change management policy<br>Vendor change management<br>Patch management<br><br>**Backup Operations, Disaster Recovery & Incident Response**<br>Disaster recovery<br>Business Continuity Plan<br>Incident response<br><br>**Vulnerability assessment**<br>External website | **1. Protect what matters**<br><br>Formalise and implement business driven and risk-based processes and procedures for protection | • Governance – Leverage existing government resources to develop a fit for purpose toolkit including strategy, framework, and policies for the sector<br>• Third parties – Develop clauses for standard tendering, procurement documentation, and certification of purchased items<br>• Supplier panel – Provide a cyber panel for purchasing of software, hardware and services<br>• Insurance coverage – Tailor insurance policy needs to risk levels | LGA<br>LG Procurement<br>LGRS<br>LG R&D Scheme | • Existing frameworks (DPC – SA Cyber Security Framework, ACSC – Essential 8 and ISM)<br>• Model policies (LGA)<br>• Advocate, assist & advance (LGA)<br>• Procurement (LGAP)<br>• ICT Vendor Panel (LGAP)<br>• Insurance (LGRS)<br>• Skytrust (LGRS)<br>• VOCAM LMS (LGRS)<br>• Examination reports (AGD)<br>• IT expertise (LGITSA)<br>• Yammer network (LGITSA)<br>• Special Interest Group (LGITSA)<br>• Conferences & workshops (LGITSA)<br>• Watch Desk (DPC)<br>• Joint operating guideline (LGSFG/DPC)<br>• Funding (LGRS, LG R&D Scheme) |
| | **2. Create a cyber aware culture**<br><br>Promote cybersecurity awareness through fit for purpose governance and an ongoing and engaging training program | • General awareness – Promote the cyber security toolkit and common terminology<br>• Training and skills development – Provide training for Executive awareness, and skills development for end users, Elected Members and IT staff<br>• Testing – Regularly assess the cyber security and policy awareness of council staff<br>• Education - Facilitate sector-wide education on cyber security threats and mitigation strategies | LGA<br>LGRS<br>LG Professionals<br>AGD | |
| | **3. Proactively identify vulnerabilities**<br><br>Tighten our monitoring and testing regimes for early identification of cybersecurity threats | • Baseline audit – Undertake audits to identify individual council improvement plans<br>• Improvement plans – Support the implementation of improvement plans to increase maturity<br>• Critical infrastructure – Identify key community infrastructure (e.g. pumping stations, traffic control, monitoring devices, etc) and certification of the systems for cybersecurity | LGRS<br>LGA | |
| | **4. Increase resilience and responsiveness**<br><br>Strengthen our ability to respond and recover from cybersecurity threats and incidents | • Threat intelligence – Form partnerships with government agencies for subscription alerts<br>• Responsiveness - Share real-time updates on threat intelligence<br>• Incidents – Develop relationships with relevant cybersecurity agencies and promote reporting of incidents, and include incident response playbooks in the cyber security toolkit | LGA<br>DPC<br>LGFSG<br>ACSC | |
| Provide ongoing guidance, support and collaboration for continuous improvement | | | | |

[1] Auditor-General Cyber Security Examinations – February 2021