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

---

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