LIYATECH EXECUTIVE READINESS SERIES

PUBLIC SERVICES, EDUCATION & COMMUNITY ORGANISATIONS CYBER READINESS CHECKLIST

Government Departments • Municipalities • Schools • Colleges • Universities • Healthcare Organisations • Trade Unions • NGOs • NPOs

"If your systems became unavailable today, how many people would lose access to essential services?"

📌 Introduction

Public service and community organisations hold some of society's most sensitive information—from citizen records and student data to patient information, member records, and community services.

Unlike many commercial organisations, a cyber incident can affect not only operations but also public confidence, service delivery, regulatory obligations, and the wellbeing of the communities you serve.

This checklist is designed to help leadership teams assess whether their organisation is prepared to protect critical information, maintain essential services, and respond effectively to today's evolving cyber risks.

Tick what applies to your organisation.

---

1. Sensitive Information & Records Protection

☐ We know where sensitive citizen, patient, student, employee, or member information is stored.

☐ Access to confidential information is limited according to roles and responsibilities.

☐ We regularly review who has access to sensitive records and information.

☐ We are confident sensitive information cannot be accessed, copied, or shared without appropriate controls.

---

2. Service Delivery & Operational Continuity

☐ We understand which systems are critical to delivering essential services.

☐ We have plans to continue operations if key systems become unavailable.

☐ Critical data is securely backed up and can be restored within acceptable timeframes.

☐ We have tested our recovery procedures for major system disruptions or cyber incidents.

---

3. Email, Fraud & Social Engineering Awareness

☐ Staff can recognise phishing emails and fraudulent requests.

☐ We have controls to reduce the risk of email impersonation and account compromise.

☐ Sensitive requests involving payments, personal information, or system access are independently verified.

☐ Staff receive regular cybersecurity awareness training.

---

4. Identity, Access & Third-Party Security

☐ Employees, contractors, and volunteers only have access to systems required for their responsibilities.

☐ User access is promptly updated or removed when individuals leave or change roles.

☐ Multi-Factor Authentication protects critical systems and accounts.

☐ Third-party service providers are granted secure and monitored access where required.

---

5. Compliance, Governance & Accountability

☐ Leadership receives regular updates on cybersecurity and information security risks.

☐ We understand our obligations regarding the protection of personal and sensitive information.

☐ Policies for information security are reviewed and updated regularly.

☐ We can demonstrate how sensitive information is protected if requested by regulators or stakeholders.

---

6. Incident Response & Organisational Resilience

☐ We have a documented cyber incident response plan.

☐ Leadership understands their responsibilities during a cyber incident.

☐ Internal and external communication procedures have been considered for major incidents.

☐ We are confident we could recover critical services while maintaining public or stakeholder confidence.

📊 Leadership Reflection

This checklist is designed to encourage leadership discussion—not to provide a score.

If several responses were **"No"** or **"Not Sure"**, it may indicate exposure in areas affecting:

• Service delivery

• Public and stakeholder trust

• Protection of personal information

• Regulatory compliance

• Organisational resilience

• Operational continuity

📞 Optional Executive Conversation

If this checklist highlighted areas of concern or uncertainty, it may be valuable to have a structured conversation about your organisation's cybersecurity and operational resilience.

The objective is to identify practical opportunities to strengthen security, improve continuity, and protect the people and communities who rely on your organisation.

Contact

Nomfundo Makapela

📧 nomfundo.makapela@liyatech.co.za

📞 073 582 4195

Terence Moabi

📧 terence.moabi@liyatech.co.za

📞 078 710 4180

🌐 www.liyatech.co.za