PILLAR FIVE

Security

Security means protecting our systems, information, and people from threats, so we can operate safely and deliver our mission with confidence.

PREVENT Stop threats before they happen

DETECT Identify threats quickly

PROTECT Protect systems and data

RESPOND Act fast when incidents occur

RECOVER Restore and learn

SCENARIO

A staff member clicks on a phishing email that looks real.

Hackers gain access and steal sensitive data.

Services are disrupted and trust is lost.

Recovery is slow and costly.

Strong security could have prevented the attack and reduced the impact.

WHAT IS SECURITY?

Security is the combination of people, processes, and technology that protects information and systems from unauthorised access, damage, disruption, or loss.

It is not just about technology – it is about building a security-aware culture and being prepared for any threat.

QUESTIONS EVERY ORGANISATION SHOULD ASK

- What are we protecting and why?
- What threats could affect us?
- Do our people understand their role in security?
- Do we control who has access to what?
- Do we have backups and recovery plans in place?
- Do we monitor and detect unusual activity?
- Do we regularly review and improve our security?

HOW TO BUILD STRONG SECURITY IN YOUR ORGANISATION

1. **Identify Risks** — Understand your assets, threats, and vulnerabilities.
2. **Put Controls in Place** — Use policies, access controls, encryption, and other safeguards to reduce risks.
3. **Train and Empower People** — Build awareness and skills so everyone can recognise and avoid threats.
4. **Monitor and Detect** — Continuously monitor systems and networks to detect suspicious activity early.
5. **Respond to Incidents** — Act quickly to contain and manage security incidents.
6. **Recover and Restore** — Restore systems and data safely and minimise disruption.
7. **Review and Improve** — Learn from incidents and continuously improve your security posture.

GOOD PRACTICE CHECKLIST

- Keep software and systems up to date.
- Use strong passwords and multi-factor authentication.
- Limit access to only what people need.
- Encrypt sensitive data.
- Back up data regularly and test backups.
- Have an incident response and recovery plan.
- Report and review incidents to learn and improve.

WARNING SIGNS

- Unusual or unexpected system activity.
- Many failed login attempts.
- Unusual emails or links from unknown senders.
- Missing or unencrypted sensitive data.
- People sharing passwords or bypassing policies.
- No backups or untested recovery plans.
- Security incidents not reported or reviewed.

Pillar Five: Security | Version 1.0 | July 2026 |