IT Security Policy

ENSEMBLE
SOLUTIONS

Effective Date: July 4, 2025

Applies To: All employees, contractors, and technology partners

1. Purpose

This policy provides clear and simple guidelines for managing technology and protecting data at Ensemble Solutions. It aims to reduce risk, maintain customer trust, and ensure operational continuity as we grow.

2. Scope

This policy applies to all staff, contractors, and vendors who access company systems, devices, or data — whether working from the office or remotely.

3. Use of IT Systems

- Company laptops, email, and cloud tools (e.g. Google Workspace, Microsoft 365, project management platforms) are for business use.
- Light personal use is acceptable if it doesn't affect productivity or pose a security risk.
- Users must not install unapproved software or bypass system protections.

4. Passwords & Access

- All accounts must be protected by strong, unique passwords.
- Multi-Factor Authentication (MFA) is required for all systems holding business or customer data.
- Access is granted based on role — only what’s needed to do your job.

5. Device Security

- Company devices must be password-protected and encrypted.
- Staff must report lost, stolen, or compromised devices to IT immediately.
- Personal devices used for work (BYOD) must have approved security settings — such as screen lock and updated software.

6. Cloud & Data Management

- We primarily use cloud services (e.g. Google Drive, OCI, AWS, etc.). These must be accessed securely and only for legitimate business purposes.
- Customer and sensitive company data must not be downloaded to personal devices without approval.
- Files must be shared using company-approved platforms only.

7. Email and Communication Security

- Watch out for phishing emails or suspicious links. If in doubt, don’t click — report it to IT.
- Don’t send customer or confidential data via email unless encrypted or shared securely (e.g. via cloud link with access control).
- Be cautious of unknown attachments or requests for login details.

8. Remote Work Guidelines

- Use secure Wi-Fi when working remotely. Avoid public networks unless using a company-approved VPN.
- Lock screens when away from your device.
- Regularly back up work to the cloud; avoid storing critical files only on local devices.

9. Software and Updates

- Only use approved apps and software tools. If you need a new tool, request it via IT.
- Enable auto-updates wherever possible to ensure software is up-to-date and secure.

10. Incident Reporting

- If something goes wrong — like a suspicious email, data breach, or device issue — report it immediately to: security@ensemblesolutions.com.au

- No blame culture: It's more important to report issues quickly so we can contain them.

11. Backups & Business Continuity

- All key data must be stored in shared cloud drives or systems that are regularly backed up.
- In the event of a system failure or outage, the team will be notified via [Phone/Email/Other] with next steps.

12. Third-Party Vendors

- Vendors or partners accessing our systems or data must meet basic security standards (e.g. secure credentials, encrypted data, no data sharing without consent).
- We use contracts or Data Processing Agreements (DPAs) where applicable.

13. Training & Awareness

- Security is everyone's responsibility.
- All team members must complete basic IT security training on joining and refresh it annually (e.g. phishing awareness, secure work practices).

14. Policy Review

- This policy will be reviewed every 12 months or after any major incident or change in operations.

15. Breach of Policy

- Breaches of this policy may lead to disciplinary action. We take security seriously to protect our customers, team, and business.

Contact

- For any questions or help, email: security@ensemblesolutions.com.au

Approved by:

Archival Garcia, Founder & CEO

Ensemble Solutions Pty Ltd

July 4, 2025