Security Working Agreement

*Last updated: Oct 8, 2025*

This document establishes the security practices [Company] has adopted to protect data, systems, and services. It provides a single reference for the rules we follow and the responsibilities we have agreed on.

# Foundation

These foundational measures establish what must be protected.

## Assets

* The IT team shall maintain an inventory of all hardware and software assets.
* The Security Officer shall maintain an inventory of the company’s sensitive data assets.

## Classifications

* The Security Officer shall create a data classification scheme defining categories of sensitivity and handling requirements for company data.

# Safeguards

These safeguards protect [Company]’s assets.

## Identity and Access

* All persons with access to sensitive company systems shall authenticate through the same central identity provider (e.g. Active Directory, Google Workspace).
* Passwords must be unique and strong, and they must not be shared.
* Where practical, systems and services shall be configured to authenticate using single sign-on (SSO) from the central identity provider.
* Multi-factor authentication (MFA) shall be required for all sensitive company systems, including the central identity provider.
* Personnel shall be granted the minimum permissions required to perform their jobs.
* User access shall be revoked promptly when staff change roles or leave.

## User Devices

* The IT department shall ensure that user devices with access to company systems:
  + Require authentication for use of the device.
  + Authenticate through the company’s primary identity provider.
  + Are configured with security protections, including full-disk encryption.
  + Run defensive software (AV/EDR) to mitigate malware risks.
  + Stay current with security updates, using automatic updates where supported.
  + Are approved by IT before use. Personal devices may be approved only if they meet these same requirements.

## Infrastructure

* The IT department shall ensure:
  + Company networks are securely configured and protected by a firewall.
  + Company Wi-Fi requires authentication using WPA2 or stronger.
  + All traffic to company systems is encrypted in transit (e.g., HTTPS or TLS).
  + Sensitive information is encrypted at rest.
  + Remote access uses secure methods (e.g., VPN or ZTNA) with MFA.
  + Company email is protected by spam and phishing filtering.

# Operations

These measures ensure resilience and reliability.

## Resilience

* The IT department shall ensure:
  + Critical business information is backed up securely and off site.
  + Critical systems generate and retain logs of security-related events.
  + System logs are reviewed regularly for signs of security issues.
* Sensitive company information shall not be shared with AI tools or services without prior approval from the Security Officer.
* The Security Officer shall maintain and test plans for restoring disrupted services.
* The Security Officer shall maintain and test plans for responding to security incidents.

## Supply Chain

* Vendors shall be assessed for security and reliability before use.
* Vendors shall be reassessed when their contracts renew or their services change.

## Governance

* Executive leadership shall appoint a Security Officer to oversee security.
* The Security Officer shall:
  + Maintain this working agreement to share with staff.
  + Ensure employees receive security awareness training.
  + Ensure staff understand their security responsibilities.
  + Promote a constructive security culture.
  + Maintain a list of security risks and review it with leadership periodically.