IT Security Policy

*[Company Name] | Effective date: [YYYY-MM-DD] | Version: 1.0*

# 1. Purpose

This IT Security Policy (“Policy”) establishes requirements to protect the confidentiality, integrity, and availability of Company information systems and data.

It aligns with relevant standards and regulations (e.g., ISO/IEC 27001, NIST CSF, POPIA/GDPR where applicable).

# 2. Scope

Applies to all employees, contractors, interns, suppliers, and third parties with access to Company systems or data.

Covers all information systems, networks, applications, devices, and cloud services used for Company business.

# 3. Roles & Responsibilities

Executive Leadership: provide resources and oversight.

Chief Information Security Officer (CISO) / Security Lead: implement and enforce this Policy, manage risk, and coordinate incident response. Contact: [security@company.com].

IT Operations: maintain secure configurations, patching, backups, and monitoring.

All Personnel: follow this Policy, complete training, and report security incidents immediately.

# 4. Information Classification & Handling

Classify data at creation: Public, Internal, Confidential, Restricted.

Handle and share data according to classification (e.g., encryption, access controls, transmission rules).

Label documents and systems appropriately; avoid storing Restricted data in unapproved locations.

# 5. Access Control & Authentication

Use the principle of least privilege and role-based access control (RBAC).

Require Multi-Factor Authentication (MFA) for privileged accounts and remote access.

Unique user accounts only—no shared passwords for production systems.

Review access at least quarterly; remove access upon role change or termination (within 24 hours).

# 6. Passwords & Secrets Management

Minimum password length: 12 characters; encourage passphrases.

Rotate credentials if compromise is suspected; otherwise rely on MFA and breach monitoring rather than frequent forced rotation.

Store secrets in an approved vault; never hardcode secrets in source code or share via email/chat.

# 7. Endpoint Security

All endpoints must run Company-approved OS versions with disk encryption enabled (e.g., BitLocker/FileVault).

Install and maintain EDR/antivirus and host-based firewall. Automatic screen lock ≤ 15 minutes idle.

Only authorized software may be installed; admin rights granted by exception and reviewed regularly.

# 8. Network Security

Segment networks by sensitivity (user, server, production, management).

Block inbound traffic by default; allow only required ports and protocols.

Use secure remote access (VPN/ZTNA) with MFA; log and monitor remote sessions.

Disable insecure protocols and ciphers; prefer TLS 1.2+ for all services.

# 9. Cloud Security

Follow least privilege IAM; no root account usage for daily operations.

Enable logging/auditing (e.g., CloudTrail/Activity Logs) and centralize logs.

Encrypt data at rest and in transit; manage keys via KMS/HSM where possible.

Harden storage (e.g., block public buckets by default); use guardrails and policies-as-code.

# 10. Application Security & SDLC

Adopt secure-by-design practices and threat modeling for significant changes.

Use code reviews, SAST/DAST/Dependency scanning in CI/CD; fix critical/high vulnerabilities before release.

Protect secrets, API keys, and tokens; rotate on exposure.

Follow change management (Section 13) for releases and infrastructure changes.

# 11. Logging, Monitoring & Alerting

Collect security-relevant logs from endpoints, servers, applications, and cloud platforms into a central system (e.g., SIEM).

Synchronize time sources; retain logs for at least [90–365] days depending on classification.

Alert on suspicious activity (e.g., failed logins, privilege escalations, unusual egress).

# 12. Vulnerability & Patch Management

Perform regular vulnerability scans (at least monthly) and penetration tests (at least annually or after major changes).

Patch timelines: Critical ≤ 7 days, High ≤ 14 days, Medium ≤ 30 days, Low as scheduled.

Document exceptions and compensating controls when patching is not immediately possible.

# 13. Change & Configuration Management

Baseline and harden system configurations; track in configuration management.

Use ticketing for changes with approval for production-affecting updates.

Maintain Infrastructure as Code (IaC) where feasible; peer review required before apply.

# 14. Backup & Recovery

Maintain backups for critical systems and data; test restores at least quarterly.

Follow 3-2-1 principle where appropriate; store backups encrypted and offsite/immutable.

Define RTO/RPO targets and ensure recovery plans meet them.

# 15. Incident Response

Report suspected incidents immediately to Security at [security@company.com] or via the hotline.

Follow the IR plan: identify, contain, eradicate, recover, and conduct post-incident review.

Notify regulators and affected parties when legally required (e.g., within POPIA/GDPR timelines).

# 16. Physical Security

Restrict access to facilities, server rooms, and network closets via badges/keys and visitor controls.

Keep work areas clear; secure documents and devices when unattended.

# 17. Remote Work & BYOD

Remote access requires MFA and compliant devices with encryption and EDR.

Personal devices (BYOD) must meet security requirements and enroll in MDM where applicable.

Prohibit storage of Restricted data on personal devices unless explicitly approved with controls.

# 18. Email, Messaging & Social Engineering

Use approved email and collaboration tools; do not forward company data to personal accounts.

Beware of phishing, smishing, and vishing; report suspicious messages using the reporting button or to Security.

Do not open unknown attachments or links; verify payment or banking changes via out-of-band methods.

# 19. Data Retention & Disposal

Retain data according to the Data Retention Schedule and legal requirements.

Sanitize or destroy media before disposal or reuse (e.g., cryptographic erase, shredding).

# 20. Third Parties & Vendors

Perform security due diligence before onboarding vendors; require contracts with security clauses, breach notification, and audit rights.

Monitor vendor performance and reassess risk periodically; control sub-processors.

# 21. Key Management & Encryption Standards

Use industry-standard algorithms and key lengths; rotate keys per policy.

Protect private keys with HSM/KMS where feasible; restrict access and log usage.

# 22. Training & Awareness

All personnel must complete security awareness training at onboarding and at least annually.

Role-based training for engineers, administrators, and high-privilege users.

# 23. Compliance & Auditing

Adhere to applicable laws and standards (e.g., POPIA, GDPR, PCI DSS where applicable).

Security conducts periodic audits; findings must be remediated within agreed timelines.

# 24. Exceptions

Exceptions require documented risk acceptance by the Security Lead/CISO and time-bound remediation plans.

# 25. Enforcement

Violations may lead to disciplinary action up to and including termination of employment, and legal action where appropriate.

# 26. Policy Review & Change History

This Policy is reviewed at least annually or upon significant changes to risk or operations.

Version 1.0 — Initial release on [YYYY-MM-DD].

*This document is uncontrolled if printed. Verify the latest version on the Company policy portal.*