Employee Cybersecurity Policy Template

Philippine business starter template

Organization	[Company / Organization Name]
Policy owner	[Department / Responsible Person]
Effective / review date	[Date] / [Review Date]

How to use this template. Set your actual password/MFA standards, name the incident-reporting channel, define BYOD and remote-work rules, and align the policy with your privacy, HR, acceptable-use and disciplinary policies.

1. Purpose

This policy establishes minimum cybersecurity requirements for employees, contractors and other authorized users of company systems and information.

2. Scope

This policy applies to company accounts, devices, networks, cloud services, websites, applications, data and any personal device authorized for company work.

3. Passwords and Authentication

- Use strong, unique passwords or passphrases for company accounts.
- Do not share passwords, MFA codes or recovery codes.
- Use company-approved password-management tools where provided.
- Enable multi-factor authentication where required or available for important accounts.
- Report unexpected MFA prompts or password-reset notices.

4. Phishing and Suspicious Messages

Do not click unexpected links, open suspicious attachments or provide credentials in response to unsolicited requests. Verify unusual payment, password-reset and account-recovery requests through a separate trusted channel.

5. Devices

- Keep company devices physically secure.
- Install required operating-system, application and security updates promptly.
- Do not disable antivirus, endpoint protection, encryption or security controls.
- Use screen locks and approved authentication.

- Report lost or stolen devices immediately.

6. Software and Downloads

Install only software, browser extensions and applications approved by the company. Pirated, unsupported or unauthorized software is prohibited.

7. Data Handling

Access company and personal data only for legitimate work purposes. Follow company rules for storage, transfer, sharing, retention and secure disposal.

8. Remote Work and Wi-Fi

Use approved remote-access methods. Avoid transmitting sensitive company data through unsecured public networks unless protected by approved security controls.

9. Personal Devices / BYOD

Personal devices used for company work must meet applicable BYOD security requirements, including screen lock, supported software, updates, access controls and remote-wipe capability where required.

10. Cloud Services and File Sharing

Use only approved cloud storage, SaaS and file-sharing services. Do not transfer company data to personal drives, personal email or unapproved collaboration tools.

11. Incident Reporting

Immediately report suspected phishing, malware, ransomware, account compromise, unauthorized access, lost devices, accidental disclosure or other security incidents to [Security Contact / Reporting Channel]. Report early even when you are unsure whether an event is serious.

12. Access Changes and Offboarding

Access rights should be changed or removed promptly when roles change or employment/engagement ends. Shared credentials should not be used as a substitute for proper user accounts.

13. Training

Personnel must complete required cybersecurity and privacy training and participate in reasonable awareness exercises appropriate to their role.

14. Compliance

Violations may result in access restrictions or corrective and disciplinary action consistent with company policy and applicable law.

Implementation Checklist

- Name the security contact and reporting channel.
- Define required MFA, password/passphrase and password-manager standards.
- Identify approved devices, browsers, software and cloud services.
- Define BYOD and remote-work controls.
- Define backup, retention and recovery responsibilities.
- Align the policy with privacy, HR, acceptable-use and disciplinary policies.
- Train employees regularly and document acknowledgement.
- Review the policy after material incidents, system changes or regulatory updates.

Important Note

This is a general starter template, not legal advice. It should be adapted to the organization's systems, contracts, industry obligations and risk profile.