Global IT Security & Data Privacy Policy

Document Version: 2.0
Effective Date: January 1, 2024
Last Revised: January 1, 2024
Document Owner: Chief Information Security Officer (CISO)
Review Cycle: Annual

---

1. Introduction

1.1 Purpose

This Global IT Security & Data Privacy Policy establishes the mandatory standards, procedures, and controls for protecting the Organization's information assets, technology infrastructure, and data privacy. The policy is designed to safeguard the confidentiality, integrity, and availability of the Company's information systems and ensure compliance with applicable laws and regulations.

1.2 Policy Statement

The Company is committed to maintaining the highest standards of information security and data privacy. All employees, contractors, consultants, temporary workers, and third parties with access to the Organization's systems and data must comply with this policy. Failure to comply may result in disciplinary action, up to and including termination of employment or contract, and potential legal action.

1.3 Information Security Objectives

The Company's information security program aims to:

- Protect confidential and sensitive information from unauthorized access, disclosure, modification, or destruction
- Ensure business continuity and minimize the impact of security incidents
- Maintain customer and stakeholder trust through responsible data stewardship
- Comply with applicable legal, regulatory, and contractual obligations
- Foster a culture of security awareness throughout the Organization

---

2. Scope and Applicability

2.1 Scope

This policy applies to:

- All information systems, networks, applications, and data owned, operated, or managed by the Company
- All devices (Company-owned and personal) used to access Company resources
- All locations where Company data is processed, stored, or transmitted
- All personnel, including full-time employees, part-time employees, contractors, consultants, temporary workers, interns, and third-party vendors

2.2 Geographic Scope

This policy applies globally to all Company operations, offices, and remote workers, regardless of geographic location.

2.3 Exclusions

There are no exclusions to this policy. All individuals with access to Company systems or data must comply with these requirements.

---

3. Definitions and Acronyms

3.1 Key Terms

- **Information Asset:** Any data, system, application, network component, or facility that has value to the Organization
- **Information Security Incident:** Any event that compromises the confidentiality, integrity, or availability of information assets
- **Authorized User:** An individual who has been granted legitimate access to Company systems and data
- **Data Subject:** An individual whose personal data is processed by the Company
- **Personal Data:** Any information relating to an identified or identifiable natural person

3.2 Acronyms

Acronym	Full Form
AUP	Acceptable Use Policy
BYOD	Bring Your Own Device
CISO	Chief Information Security Officer
DLP	Data Loss Prevention
GDPR	General Data Protection Regulation
HR	Human Resources
IAM	Identity and Access Management
IoT	Internet of Things
IR	Incident Response
ISMS	Information Security Management System
IT	Information Technology
MFA	Multi-Factor Authentication
MDM	Mobile Device Management
PDPA	Personal Data Protection Act (Thailand)
P2P	Peer-to-Peer
VPN	Virtual Private Network
2FA	Two-Factor Authentication (same as MFA)

4. Access Control and Authentication

4.1 User Account Management

4.1.1 Account Provisioning

- All user accounts must be formally requested and approved through the IT Service Desk ticketing system

- Account access must be based on the principle of least privilege (minimum necessary access to perform job functions)
- New employee accounts shall be provisioned only after receipt of written authorization from HR and the employee's direct manager
- All accounts must be linked to a specific individual; shared or generic accounts are strictly prohibited except for specific technical service accounts (which require CISO approval)
- Default passwords must be changed immediately upon first login

4.1.2 Account Deprovisioning

- User accounts must be disabled immediately upon termination, resignation, or extended leave (>30 days)
- HR must notify IT Security within 2 hours of employee termination
- Manager must notify IT Security immediately when an employee changes roles or departments
- Access rights must be reviewed and adjusted within 24 hours of role change
- Dormant accounts (no login activity for 90 days) will be automatically disabled and flagged for review

4.2 Password Policy

All users must comply with the following password requirements to ensure strong authentication security.

4.2.1 Password Complexity Requirements

Mandatory Standards:

Requirement	Specification	Rationale
Minimum Length	12 characters	Provides sufficient entropy against brute-force attacks
Character Composition	Must contain characters from at least 3 of the following 4 categories:• Uppercase letters (A-Z)• Lowercase letters (a-z)• Numbers (0-9)• Special characters (!@#$%^&*()_+-=[]{};|:<>?,./)	Increases password complexity and resistance to dictionary attacks
Password Expiration	90 days	Regular rotation reduces the risk from compromised credentials

Password History	Cannot reuse the last 5 passwords	Prevents users from cycling through a small set of passwords
Account Lockout	Account locks after 5 failed login attempts within 15 minutes	Protects against automated password guessing attacks
Lockout Duration	30 minutes or until IT/Manager unlocks	Balances security with user convenience

4.2.2 Prohibited Password Practices

Users must NOT:

- Use passwords that contain their username, real name, or company name
- Use dictionary words, common phrases, or sequential patterns (e.g., "Password123", "Qwerty123!", "123456789")
- Share passwords with anyone, including supervisors, IT staff, or family members
- Write down passwords or store them in unencrypted files
- Use the same password across multiple systems or services (including personal accounts)
- Store passwords in web browsers without additional encryption (use approved password managers only)
- Disclose passwords over email, phone, instant messaging, or in any other unsecured manner

4.2.3 Password Manager Requirements

- Employees are encouraged to use approved password management software (e.g., 1Password, LastPass Enterprise, Bitwarden)
- Password managers must be configured with a strong master password that meets or exceeds the complexity requirements above
- Password manager databases should be backed up regularly and secured with encryption

4.2.4 Administrative and Privileged Account Passwords

- Administrative accounts (domain admin, root, database admin) must use passwords with a minimum of **16 characters**
- Privileged account passwords must be changed every **60 days** (more frequently than standard user accounts)
- Privileged account credentials must be stored in a secure password vault (e.g., CyberArk, HashiCorp Vault) with access logging
- All privileged access must be logged and reviewed quarterly by IT Security

4.3 Multi-Factor Authentication (MFA)

4.3.1 MFA Requirements

Mandatory MFA for:

Access Type	MFA Requirement	Implementation
Remote Access (VPN)	**MANDATORY - No exceptions**	All VPN connections must authenticate using MFA before establishing connection
Email (External Access)	**MANDATORY**	Webmail and mobile email access from outside the corporate network
Cloud Services	**MANDATORY**	All SaaS applications (Office 365, Google Workspace, Salesforce, AWS, etc.)
Administrative Accounts	**MANDATORY**	All privileged accounts must use MFA for every login
Financial Systems	**MANDATORY**	Access to accounting, payroll, and financial management systems
On-premise Access	**RECOMMENDED**	Strongly recommended but not required for workstations on the corporate network

4.3.2 Approved MFA Methods

The Company supports the following MFA methods (listed in order of security strength):

1. **Hardware Security Keys** (Preferred)
    - YubiKey, Titan Security Key, or equivalent FIDO2-compliant devices
    - Provides the highest level of security against phishing
2. **Authenticator Apps** (Recommended)
    - Microsoft Authenticator, Google Authenticator, Authy, Duo Mobile
    - Generates time-based one-time passwords (TOTP)
3. **Push Notifications** (Acceptable)
    - Duo Push, Microsoft Authenticator push approval
    - Convenient but requires user vigilance against push fatigue attacks

4. **SMS/Text Message** (Acceptable as fallback only)

    - One-time codes sent via SMS
    - Less secure due to SIM swapping risks; should only be used when other methods are unavailable

Prohibited MFA Methods:

- Email-based one-time codes (vulnerable to email compromise)
- Voice calls for MFA codes (vulnerable to social engineering)

4.3.3 MFA Device Management

- Users must register at least **two MFA devices** (primary and backup) to prevent account lockout
- Lost or stolen MFA devices must be reported immediately to IT Security
- MFA device changes require identity verification before re-registration
- Emergency access procedures (MFA bypass) require approval from the user's manager and CISO

4.4 Access Review and Recertification

- All user access rights must be reviewed and recertified by managers on a **quarterly basis**
- IT Security will provide access reports to managers for review
- Managers must confirm that each user's access is appropriate for their current role
- Any discrepancies must be reported and remediated within 5 business days
- Failure to complete access reviews may result in automatic suspension of non-reviewed accounts

5. Device Management and BYOD Policy

5.1 Device Management Overview

The Company recognizes that employees may use personal devices to access corporate resources. To balance productivity with security, the Organization has established a Bring Your Own Device (BYOD) program with mandatory security controls.

5.2 BYOD Program Eligibility and Enrollment

5.2.1 Eligible Devices

The following personal devices may be enrolled in the BYOD program:

- Smartphones (iOS 15.0 or higher, Android 11 or higher)
- Tablets (iPad OS 15.0 or higher, Android 11 or higher)
- Laptops (Windows 10/11 Pro, macOS 12.0 or higher, approved Linux distributions)

Ineligible Devices:

- Jailbroken or rooted devices
- Devices running unsupported or end-of-life operating systems
- Devices with known security vulnerabilities that cannot be patched
- Devices shared with family members or other individuals

5.2.2 Enrollment Requirements

To enroll a personal device in the BYOD program, employees must:

1. Complete and sign the **BYOD Acknowledgment and Consent Form**
2. Install and configure the Company's approved **Mobile Device Management (MDM)** software
3. Ensure the device meets minimum security requirements (see Section 5.3)
4. Undergo device security validation by IT Security before accessing Company resources
5. Agree to periodic security assessments and remote management by IT Security

5.2.3 Voluntary Participation

- BYOD participation is voluntary; employees who prefer not to enroll personal devices will be issued Company-owned devices
- Employees may unenroll from BYOD at any time by notifying IT Security and uninstalling the MDM software
- Upon unenrollment, all Company data will be removed from the device

5.3 Mandatory Device Security Requirements

5.3.1 MDM Installation and Configuration

Mobile Device Management (MDM) Requirements:

Requirement	Specification	Purpose
MDM Software	Must install Company-approved MDM solution (Microsoft Intune, VMware Workspace ONE, or equivalent)	Enables centralized security management and policy enforcement
MDM Profile	Must maintain active MDM profile at all times	Allows IT to push security configurations and monitor compliance
Remote Management	Must allow remote device management including remote wipe capability	Enables protection of Company data in case of device loss or theft
Compliance Monitoring	Device compliance status checked every 24 hours	Ensures ongoing adherence to security requirements

Important: The MDM software only manages the work profile or work-related applications. Personal data, photos, messages, and applications outside the work profile remain private and are not accessible to the Company.

5.3.2 Device Security Controls

All BYOD devices must comply with the following security controls:

Control	Requirement	Enforcement
Device Encryption	Full-disk/device encryption must be enabled	Mandatory - MDM enforced
Screen Lock	PIN, password, fingerprint, or face recognition requiredMinimum 6-character PIN/password	Mandatory - MDM enforced
Auto-Lock Timeout	Maximum 5 minutes of inactivity	Mandatory - MDM enforced
OS Updates	Operating system must be updated to the latest security patches within 30 days of release	Mandatory - MDM monitored

Antivirus/Anti-malware	Required on all laptops and Windows devicesCompany-approved solution must be installed and updated	Mandatory - MDM enforced
Firewall	Personal firewall must be enabled	Mandatory - MDM enforced
Bluetooth Security	Bluetooth must be disabled when not in useBluetooth discoverability must be turned off	Strongly recommended
Wi-Fi Security	No connections to open/unsecured Wi-Fi networks when accessing Company dataVPN required on untrusted networks	Mandatory - User responsibility
App Installation	Only install apps from official stores (Apple App Store, Google Play Store)Sideloading apps prohibited	Mandatory - User responsibility

5.3.3 Prohibited Device Configurations

The following configurations will result in immediate device blocking and revocation of access:

- Jailbroken (iOS) or rooted (Android) devices
- Devices with MDM profiles removed or tampered with
- Devices with developer mode enabled (unless explicitly approved for development work)
- Devices with USB debugging enabled (Android)
- Devices with unknown sources installation enabled (Android)
- Devices running pirated or unlicensed operating systems

5.4 Device Loss, Theft, or Compromise

5.4.1 Immediate Reporting Requirement

CRITICAL: Any employee whose device is lost, stolen, or suspected of being compromised MUST report the incident within 4 hours of discovery.

Reporting Channels (available 24/7):

- IT Security Hotline: [Phone Number]
- IT Security Email: security@company.com
- Emergency Response Portal: [URL]

5.4.2 Incident Report Information

When reporting a lost or stolen device, provide the following information:

- Date, time, and location where device was last seen
- Device type, manufacturer, and model
- Device serial number or IMEI (if known)
- Last known activities performed on the device
- Sensitivity of data stored on or accessible from the device
- Whether device has screen lock enabled
- Whether device is enrolled in MDM

5.4.3 Company Response Actions

Upon receipt of a device loss/theft report, IT Security will:

1. **Immediately (within 15 minutes):**
    - Initiate remote device lock via MDM
    - Disable user account access to prevent unauthorized access
    - Generate alert to security operations team
2. **Within 1 hour:**
    - Attempt device location tracking (if enabled and legal)
    - Assess data exposure risk based on device content
    - Notify user's manager and HR (for potential breach notification obligations)
3. **Within 4 hours:**
    - If device cannot be located and risk is high: Initiate remote wipe of all Company data
    - Document incident in security incident log
    - Begin incident investigation
4. **Within 24 hours:**
    - Complete incident assessment
    - Determine if regulatory breach notification is required
    - Provide incident report to CISO

5.4.4 Employee Responsibilities After Device Loss

After reporting device loss/theft, employees must:

- File a police report (required for theft; provide copy to IT Security)
- Change passwords for all accounts accessed from the lost device
- Monitor personal accounts for suspicious activity
- Not attempt to remotely access or locate the device (leave this to IT Security)

- Cooperate fully with incident investigation
- If device is recovered, do not use it until IT Security performs a security assessment

5.4.5 Consequences of Late Reporting

Failure to report device loss/theft within 4 hours may result in:

- Formal written warning for first offense
- Suspension without pay for second offense
- Termination of employment for third offense or if data breach occurs due to delayed reporting
- Personal liability for any data breach costs resulting from delayed reporting

5.5 Personal vs. Company Data Separation

- The Company will use containerization technology to separate work data from personal data
- Only data within the work container is subject to Company policies and remote management
- Personal data (photos, personal emails, personal apps, contacts) remains private
- Upon device unenrollment or employment termination, only the work container is wiped; personal data remains intact

5.6 Data Roaming and International Travel

- Data roaming should be disabled unless required for business purposes
- Employees traveling internationally with BYOD devices must notify IT Security 48 hours in advance
- Additional security controls may be required for travel to high-risk countries
- Devices must connect through Company VPN when accessing Company resources from abroad

5.7 Company-Owned Devices

Company-owned devices are subject to more stringent controls:

- All company-owned devices must be enrolled in MDM with full management capabilities
- Company reserves the right to monitor all activity on company-owned devices
- No expectation of privacy on company-owned devices
- Personal use of company devices should be minimal and comply with Acceptable Use Policy
- Company-owned devices must be returned immediately upon termination or resignation

6. Data Classification and Handling

6.1 Data Classification Framework

The Company classifies all information assets into four levels based on sensitivity, legal/regulatory requirements, and potential impact if compromised. All employees must understand these classifications and handle data appropriately.

6.2 Classification Levels

6.2.1 Classification Summary Table

Classification Level	Definition	Examples	Impact of Unauthorized Disclosure
PUBLIC	Information intended for public consumption	Marketing materials, published press releases, public website content, job postings	Minimal or no impact
INTERNAL	Information for internal use; not sensitive but not intended for public	Internal policies, organizational charts, internal newsletters, general business communications	Low impact; may cause minor embarrassment or competitive disadvantage
CONFIDENTIAL	Sensitive information that could harm the Company or individuals if disclosed	Employee personal data, customer information, financial reports, business strategies, vendor contracts	Moderate to significant impact; could result in competitive disadvantage, regulatory penalties, or reputational damage
RESTRICTED	Highly sensitive information requiring the highest level of protection	Trade secrets, encryption keys, authentication credentials, strategic M&A plans, unreleased financial data, personal health information, payment card data	Severe impact; could result in significant financial loss, legal liability, regulatory sanctions, loss of competitive advantage, or harm to individuals

6.2.2 Data Classification Criteria

PUBLIC Data

- Approved for public disclosure
- No confidentiality concerns
- Available on public website or public channels
- No special handling requirements

INTERNAL Data

- For company employees and authorized contractors only
- Not approved for external distribution
- Could cause minor inconvenience if disclosed
- Requires basic access controls

CONFIDENTIAL Data

- Restricted to authorized personnel with business need-to-know
- Subject to privacy laws or regulatory requirements (GDPR, PDPA, etc.)
- Could cause significant harm to the Company or individuals if compromised
- Requires strong access controls and encryption

RESTRICTED Data

- Extremely limited distribution - only specific individuals with explicit authorization
- Subject to strict legal, regulatory, or contractual protection requirements
- Could cause severe or catastrophic damage if compromised
- Requires the strongest possible security controls

6.3 Data Labeling Requirements

6.3.1 Document Labeling

All documents containing CONFIDENTIAL or RESTRICTED data must be clearly labeled:

- **Digital Documents:** Include classification level in header or footer (e.g., "CONFIDENTIAL - Internal Use Only")
- **Email:** Include classification in subject line (e.g., "[RESTRICTED] Q4 Financial Results")
- **Presentations:** Include classification on title slide and footer of all slides
- **Printed Documents:** Mark classification prominently on first page and each subsequent page

6.3.2 Data Classification Responsibilities

Role	Responsibility
Data Owner	Executive or senior manager responsible for the business function that creates/manages the data• Assigns initial classification level • Approves access to CONFIDENTIAL/RESTRICTED data • Reviews and updates classification annually
Data Custodian	IT staff responsible for technical implementation of security controls • Implements access controls according to classification • Maintains security controls and monitors compliance • Reports security incidents to Data Owner
Data User	All employees who create, access, or handle data • Classifies data appropriately when creating new information • Handles data according to its classification level • Reports suspected misclassification or security incidents

6.4 Handling Requirements by Classification Level

6.4.1 PUBLIC Data Handling

Access: Unrestricted

Storage:

- May be stored on any company-approved system
- No encryption required (but recommended)

Transmission:

- May be transmitted via any means including unencrypted email
- May be shared on public websites and social media

Disposal:

- Standard deletion or recycling acceptable

6.4.2 INTERNAL Data Handling

Access: Company employees and authorized contractors with valid business need

Storage:

- Must be stored on company-approved systems only
- No storage on personal devices unless enrolled in BYOD with MDM
- Basic access controls required (user authentication)

Transmission:

- Email transmission within company domain acceptable
- External transmission requires business justification
- No posting on public websites or social media

Disposal:

- Standard secure deletion
- Recycling of printed materials acceptable after verifying content is illegible

6.4.3 CONFIDENTIAL Data Handling

Access: Limited to authorized individuals with explicit business need-to-know

Storage:

- Must be stored on company-approved systems with access controls
- Encryption required for portable devices (laptops, USB drives)
- Cloud storage only in approved services with encryption (OneDrive for Business, SharePoint, approved cloud providers)
- No storage on personal devices unless in encrypted work container with MDM

Transmission:

- Email transmission must use encryption (Office 365 Encryption, S/MIME, or PGP)
- File sharing only through approved encrypted channels (encrypted SharePoint links, secure file transfer)
- External sharing requires approval from Data Owner and must use encryption
- Must use VPN when accessing over untrusted networks

Disposal:

- Secure deletion with data wiping software (minimum 3-pass overwrite)
- Physical documents must be cross-cut shredded (minimum 2mm x 15mm particles)
- Hard drives and storage media must be degaussed or physically destroyed before disposal

Additional Controls:

- Document access logging enabled
- Regular access reviews by Data Owner
- Data Loss Prevention (DLP) policies enforced

6.4.4 RESTRICTED Data Handling

Access: Extremely limited - requires explicit written authorization from Data Owner or CISO

Storage:

- Must be stored in highly secure, access-controlled systems with audit logging
- Encryption mandatory at rest and in transit (minimum AES-256 or equivalent)
- Must use dedicated secure storage solutions with enhanced monitoring
- Absolutely NO storage on personal devices under any circumstances
- No storage on removable media (USB drives, external drives) except with CISO approval and full-disk encryption

Transmission:

- Transmission only through encrypted channels with strong authentication
- External transmission requires CISO approval and must use end-to-end encryption
- Must use secure file transfer protocols (SFTP, encrypted email with PGP/S/MIME)
- Must use VPN for any remote access
- No transmission via public cloud services unless specifically approved and encrypted
- Large file transfers must use approved secure file transfer service with access controls

Access Controls:

- Multi-factor authentication (MFA) mandatory for all access
- All access must be logged and reviewed monthly
- Privileged Access Management (PAM) required for administrative access
- Role-based access control (RBAC) strictly enforced

Disposal:

- Cryptographic shredding (encryption keys destroyed) or minimum 7-pass secure wipe
- Physical media must be physically destroyed (incinerated, crushed, or degaussed)
- Certificate of destruction required for all disposed media
- Third-party disposal services must be certified (e.g., NAID AAA Certified)

Additional Controls:

- Data Loss Prevention (DLP) rules enforced with blocking enabled
- Watermarking required on printed documents and some digital documents

- Screen capture and print functions may be disabled
- Activity monitoring and behavioral analytics
- No email forwarding or copying to external accounts
- Annual access recertification mandatory

Special Handling:

- RESTRICTED data must not be discussed in public areas
- Video/audio conferencing about RESTRICTED topics must use encrypted platforms only
- Printed RESTRICTED documents must be kept in locked storage when not in active use
- Work involving RESTRICTED data should be performed in secure areas when possible

6.5 Data Reclassification and Declassification

- Data classification must be reviewed annually by the Data Owner
- Data may be reclassified to a lower level only with written approval from Data Owner
- Data may be declassified (downgraded to PUBLIC) only after legal and compliance review
- All changes in classification must be documented and communicated to affected users

6.6 Third-Party Data Sharing

- Sharing CONFIDENTIAL or RESTRICTED data with third parties requires a signed Non-Disclosure Agreement (NDA) or Data Processing Agreement (DPA)
- Third-party access must be limited to minimum necessary data
- Third-party security controls must be assessed before granting access
- Third-party access must be reviewed quarterly and revoked when no longer needed

7. Acceptable Use Policy (AUP)

7.1 Purpose and Scope

This Acceptable Use Policy defines the acceptable and unacceptable uses of the Company's information technology resources, including but not limited to computers, networks, internet access, email systems, software, mobile devices, and cloud services.

All users of Company IT resources must comply with this policy. Violation of this policy may result in disciplinary action up to and including termination of employment or contract, and may expose the violator to civil or criminal liability.

7.2 General Acceptable Use Principles

7.2.1 Business Purpose

Company IT resources are provided primarily for business purposes. Limited personal use is permitted under the following conditions:

- Personal use must not interfere with work responsibilities or productivity
- Personal use must not consume significant system resources or network bandwidth
- Personal use must comply with all policies, including security and confidentiality requirements
- Personal use must not involve any prohibited activities (see Section 7.3)
- Personal use must not create legal liability or reputational risk for the Company

7.2.2 Authorized Access Only

- Users may only access systems, applications, and data for which they have explicit authorization
- Users must not attempt to access or use another user's account, password, or data without authorization
- Users must not attempt to bypass, disable, or circumvent security controls
- Unauthorized access attempts, including "curiosity browsing," are strictly prohibited

7.2.3 Professional and Ethical Conduct

- Users must conduct themselves professionally when using Company IT resources
- Users must respect intellectual property rights and comply with software licensing agreements
- Users must respect the privacy of others and not access, copy, or share others' personal information without authorization
- Users must not create, transmit, or display offensive, discriminatory, harassing, or illegal content

7.3 Prohibited Activities

The following activities are strictly prohibited when using Company IT resources:

7.3.1 Prohibited Software and Technologies

Prohibited Technology	Description	Rationale	Enforcement
Peer-to-Peer (P2P) File Sharing Software	BitTorrent, uTorrent, LimeWire, Kazaa, eMule, or any similar P2P file sharing applications	• Significant security risk (malware distribution) • Copyright infringement risk • Network performance degradation • Potential legal liability	**Immediate termination of employment for installation or use**Blocked at network level
Tor Browser and Anonymization Tools	Tor Browser, Tor network, Freenet, I2P, or any anonymization/darknet tools	• Bypasses security controls and monitoring • Associated with illegal activities • Prevents DLP and security monitoring • Circumvents acceptable use policies	**Immediate termination of employment for installation or use**Blocked at network level
VPN Services (Unauthorized)	Personal VPN services (NordVPN, ExpressVPN, etc.) that are not company-approved	• Bypasses network security controls • Prevents content filtering and monitoring • Potential data exfiltration channel	**Written warning for first offenseTermination for repeat offense**Blocked at network level

Remote Access Tools (Unauthorized)	TeamViewer, AnyDesk, LogMeIn (personal accounts), Chrome Remote Desktop for personal use	• Creates unmonitored access pathways • Potential data exfiltration risk • Bypasses access controls	**Written warning for first offenseTermination for repeat offense**Requires IT approval
Cryptocurrency Mining Software	Any cryptocurrency mining application or browser-based mining scripts	• Consumes excessive system resources • Degrades system performance • Increases electricity costs • Potential malware vector	**Immediate termination of employment**Blocked at network level
Hacking and Penetration Tools (Unauthorized)	Metasploit, Kali Linux tools, password cracking tools, network scanners (except for authorized security personnel)	• Can be used for malicious purposes • Creates security incidents • Legal liability risk	**Immediate termination of employment unless authorized by CISO for legitimate security work**
Pirated or Unlicensed Software	Any software obtained through unauthorized channels or without proper licensing	• Copyright infringement • Legal liability • Security risks (often bundled with malware) • Audit compliance issues	**Immediate termination of employmentCompany may pursue legal action**

Software Installation Requirements:

- All software installations require IT approval through the service desk ticketing system
- Only software from approved vendors and official sources may be installed
- Software must be properly licensed with valid licenses assigned to specific users
- Freeware and open-source software require security review before installation

7.3.2 Prohibited Content and Communications

Absolutely Prohibited:

The following types of content must never be created, stored, transmitted, or accessed using Company IT resources:

- **Illegal Content:** Child pornography, illegal drugs, terrorism-related materials, or any content that violates local, national, or international laws
- **Malicious Software:** Viruses, worms, Trojans, ransomware, spyware, or any malicious code
- **Offensive Content:** Pornography, sexually explicit materials, extreme violence, hate speech, discriminatory content
- **Harassment or Discrimination:** Content that harasses, threatens, demeans, or discriminates based on race, ethnicity, gender, religion, sexual orientation, age, disability, or any protected characteristic
- **Confidential Information of Others:** Trade secrets or confidential information belonging to previous employers or other organizations (without proper authorization)
- **False or Misleading Information:** Intentionally false, defamatory, or misleading content about the Company, colleagues, competitors, or others

7.3.3 Prohibited Network Activities

- **Denial of Service Attacks:** Intentionally disrupting network services or overwhelming systems
- **Packet Sniffing:** Intercepting or monitoring network traffic without authorization
- **Port Scanning:** Scanning networks or systems for vulnerabilities without authorization
- **Spoofing:** Impersonating another user, system, or email address
- **Unauthorized Network Bridging:** Connecting Company networks to external networks without authorization
- **Wireless Access Point Installation:** Installing unauthorized Wi-Fi access points or routers

7.4 Internet and Web Usage

7.4.1 Acceptable Internet Use

- Internet access is provided primarily for business purposes
- Reasonable personal use during breaks is acceptable if it complies with policy
- Users should use discretion and common sense when accessing internet content
- Users are reminded that internet activity is monitored and logged

7.4.2 Restricted or Prohibited Websites

The following categories of websites are blocked or restricted:

Category	Access Level	Rationale
Adult Content / Pornography	**Blocked**	Inappropriate; creates hostile work environment
Gambling	**Blocked**	Legal risk; productivity concern
Illegal Drugs	**Blocked**	Illegal activity; policy violation
Weapons	**Blocked**	Workplace safety concern
Hate Speech / Discrimination	**Blocked**	Hostile work environment; policy violation
Malware / Phishing	**Blocked**	Security threat
P2P / File Sharing	**Blocked**	Security risk; legal liability
Anonymization / Proxy	**Blocked**	Security control bypass
Hacking / Security Tools	**Restricted**	Allowed only for authorized security personnel
Job Search / Recruitment	**Monitored**	Excessive use may indicate performance issues
Streaming Media	**Restricted**	Bandwidth management; productivity
Personal Email (Webmail)	**Monitored**	Potential data exfiltration; acceptable for limited personal use
Social Media	**Monitored**	See Section 7.5 for detailed policy

7.4.3 Bypassing Content Filters

- Users must not attempt to bypass or circumvent web content filters, firewalls, or security controls
- Using proxy servers, VPNs, or translation services to access blocked content is prohibited
- Violations will result in disciplinary action up to and including termination

7.5 Social Media Usage Guidelines

7.5.1 Personal Social Media Use at Work

Permitted:

- Limited personal use of social media during breaks and lunch periods
- Accessing personal accounts for brief periods if it does not interfere with work

Not Permitted:

- Excessive time spent on social media during work hours
- Posting confidential company information or trade secrets
- Posting disparaging comments about the Company, colleagues, customers, or competitors
- Posting content that violates the Company's harassment, discrimination, or code of conduct policies
- Impersonating the Company or suggesting official endorsement without authorization

7.5.2 Business Use of Social Media

If you are authorized to post on behalf of the Company:

- Follow all brand guidelines and obtain necessary approvals before posting
- Clearly identify yourself as a Company representative when appropriate
- Be professional, accurate, and respectful in all communications
- Do not disclose confidential information, financial data, or business strategies
- Respond to negative comments professionally; escalate serious issues to Marketing/PR
- Comply with all applicable laws and regulations (FTC guidelines, GDPR, etc.)

7.5.3 Personal Social Media Best Practices

When posting on personal social media, employees should:

- Include a disclaimer if discussing topics related to the Company or industry: "Views are my own and do not represent my employer"
- Avoid posting photos or videos taken at work without permission
- Be mindful that personal social media activity may reflect on the Company
- Report any suspicious messages or potential phishing attempts to IT Security

7.5.4 Prohibited Social Media Activities

- Posting confidential information, trade secrets, or non-public financial information
- Posting offensive, discriminatory, or harassing content
- Cyberbullying, trolling, or engaging in online harassment
- Sharing customer data or personal information without consent

- Engaging in illegal activities or encouraging others to do so
- Using Company social media accounts for personal benefit or political campaigning

7.6 Email Usage

7.6.1 Acceptable Email Use

- Company email is provided for business communication
- Limited personal use is acceptable if it does not interfere with work responsibilities
- Users must comply with professional communication standards
- Users are reminded that all email is subject to monitoring and may be disclosed in legal proceedings

7.6.2 Email Security Requirements

- Do not open attachments or click links from unknown or suspicious senders
- Verify unexpected emails from known senders before opening attachments (potential phishing)
- Do not forward company email to personal email accounts
- Use encryption for sensitive information (CONFIDENTIAL or RESTRICTED data)
- Use BCC (blind carbon copy) when sending to large distribution lists to protect privacy
- Configure out-of-office messages appropriately (do not include detailed schedule or confidential information)

7.6.3 Prohibited Email Activities

- Sending chain letters, spam, or unsolicited commercial email
- Sending large attachments that could impact system performance (>25MB without approval)
- Using email for personal business ventures or solicitations
- Forwarding confidential information to unauthorized recipients
- Creating or forwarding emails containing offensive, discriminatory, or harassing content
- Email spoofing or impersonating another person

7.7 Cloud Services and File Sharing

7.7.1 Approved Cloud Services

The Company has approved the following cloud services for business use:

- Microsoft Office 365 (OneDrive for Business, SharePoint Online, Teams)
- Google Workspace (if applicable to your department)
- [Other approved services as documented by IT]

7.7.2 Prohibited Cloud Services

The following practices are prohibited:

- Using personal cloud storage (personal Dropbox, Google Drive, iCloud, etc.) for Company data
- Uploading CONFIDENTIAL or RESTRICTED data to unauthorized cloud services
- Sharing Company data through personal file-sharing services (WeTransfer, SendAnywhere, etc.)
- Using cloud services in countries subject to data sovereignty restrictions without approval

7.8 Mobile Device Usage

7.8.1 Company-Issued Mobile Devices

- Provided primarily for business communication
- Limited personal use acceptable
- Must comply with device security requirements (Section 5)
- Must not be used while driving (hands-free only)

7.8.2 Personal Mobile Devices (BYOD)

- Must be enrolled in MDM program to access Company resources
- Must comply with all security requirements (Section 5)
- Must not be used to photograph confidential documents or screens without authorization
- Must not be used to record audio/video in the workplace without consent

7.9 Monitoring and Privacy

7.9.1 Company's Right to Monitor

The Company reserves the right to monitor all use of IT resources, including but not limited to:

- Network traffic and internet browsing history
- Email content and metadata
- File access and transfers
- Application usage
- System logs and authentication events
- Mobile device activity (for devices enrolled in MDM)
- Voice and video communications on Company systems

7.9.2 No Expectation of Privacy

- Users have no expectation of privacy when using Company IT resources
- All data stored on Company systems is considered Company property
- Monitoring may be conducted without prior notice
- Information collected through monitoring may be used for security investigations, policy enforcement, or legal proceedings

7.9.3 Privacy Considerations

- The Company will make reasonable efforts to respect employee privacy
- Personal data collected through monitoring will be handled in accordance with privacy laws
- Monitoring data will be accessed only by authorized personnel for legitimate business purposes
- Employees will be notified of monitoring practices through this policy and other communications

7.10 Violations and Enforcement

Violations of this Acceptable Use Policy will be investigated and may result in:

- Verbal or written warning
- Suspension of IT access privileges
- Mandatory security awareness training
- Formal performance improvement plan
- Suspension without pay
- Termination of employment
- Legal action and referral to law enforcement (for illegal activities)

The severity of the consequence will depend on the nature and severity of the violation, intent, and the employee's prior disciplinary record.

8. Incident Response and Reporting

8.1 Information Security Incidents

An information security incident is any event that actually or potentially jeopardizes the confidentiality, integrity, or availability of information assets or violates security policies.

8.2 Types of Security Incidents

Common security incidents include:

- **Phishing and Social Engineering:** Suspicious emails, phone calls, or messages attempting to steal credentials or information
- **Malware Infections:** Viruses, ransomware, spyware, or other malicious software detected on systems
- **Unauthorized Access:** Attempts to access systems or data without authorization
- **Data Breaches:** Unauthorized disclosure, access, or loss of sensitive data
- **Lost or Stolen Devices:** Missing laptops, mobile devices, USB drives, or other media containing Company data
- **Account Compromise:** Suspected or confirmed unauthorized access to user accounts
- **Denial of Service:** Disruption of system availability or network services
- **Insider Threats:** Malicious or negligent actions by employees or contractors
- **Physical Security Breaches:** Unauthorized physical access to facilities or data centers

8.3 Incident Reporting Requirements

8.3.1 Mandatory Reporting

ALL security incidents, suspected incidents, or potential vulnerabilities MUST be reported immediately.

- Do not delay reporting while investigating on your own
- Do not assume someone else has already reported the incident
- When in doubt, report it - it is better to report a non-incident than to fail to report a real incident
- Failure to report a security incident is a policy violation and may result in disciplinary action

8.3.2 Reporting Channels

24/7 Security Operations Center (SOC):

- **Email:** security@company.com (monitored 24/7)
- **Phone:** [Security Hotline Number] (24/7 hotline)
- **Web Portal:** [Incident Reporting Portal URL]
- **Instant Message:** IT Security channel on Microsoft Teams / Slack

For emergencies outside business hours or if primary channels are unavailable:

- **CISO Mobile:** [Mobile Number]
- **IT Director Mobile:** [Mobile Number]

8.3.3 Reporting Timeframes

Incident Type	Reporting Timeframe
Critical Incidents (active data breach, ransomware, system compromise)	**Immediately** (within 15 minutes)
High Severity (suspected compromise, lost device with sensitive data, confirmed phishing attack)	**Within 1 hour**
Medium Severity (suspicious activity, potential malware, policy violations)	**Within 4 hours**
Low Severity (minor policy violations, informational reports)	**Within 24 hours**

8.4 Phishing and Social Engineering Response

8.4.1 Recognizing Phishing Attempts

Common indicators of phishing emails:

- **Sender Address Spoofing:** Email address looks similar but not identical to legitimate address (e.g., "admin@c0mpany.com" instead of "admin@company.com")
- **Urgent or Threatening Language:** "Your account will be suspended," "Immediate action required," "Verify within 24 hours"
- **Requests for Credentials:** Legitimate companies will never ask for passwords via email
- **Suspicious Links:** Hover over links to reveal the actual URL before clicking
- **Generic Greetings:** "Dear Customer" instead of using your actual name
- **Grammar and Spelling Errors:** Poor language quality or unusual phrasing
- **Unexpected Attachments:** Particularly .exe, .zip, .scr files from unknown senders
- **Too Good to Be True Offers:** Prize notifications, lottery winnings, unexpected refunds

8.4.2 If You Receive a Suspicious Email

DO:

1. **Do not click any links or open attachments**
2. **Do not reply to the email**
3. **Report the email immediately:**
    - Forward the suspicious email as an attachment to: security@company.com
    - Or use the "Report Phishing" button in Outlook/Gmail
    - Include a brief description of why you find it suspicious
4. **Delete the email** from your inbox after reporting

DO NOT:

- Do not forward the phishing email to colleagues (except to IT Security)
- Do not try to "test" if the link is malicious by clicking it
- Do not engage with the sender or attempt to investigate yourself
- Do not ignore it - even if you think it's obviously fake, report it

8.4.3 If You Clicked a Suspicious Link or Opened an Attachment

Immediate Actions (within 5 minutes):

1. **Do not panic, but act quickly**
2. **Disconnect from the network:**
    - Unplug Ethernet cable or disable Wi-Fi
    - Do NOT shut down the computer (this may destroy evidence)
3. **Call IT Security immediately:** [Security Hotline]
4. **Do not attempt to remove malware yourself**

After Contacting IT Security:

5. **Change passwords** for all critical accounts from a different, clean device:
    - Email account
    - VPN account
    - Any financial or administrative systems you have access to
    - Enable MFA if not already enabled
6. **Monitor accounts** for suspicious activity
7. **Complete an incident report** through the security portal
8. **Cooperate fully** with IT Security investigation

8.4.4 If You Provided Credentials or Sensitive Information

Critical - Immediate Actions (within 5 minutes):

1. **Call IT Security immediately:** [Security Hotline] - do not wait
2. **Change your password immediately** from a different, secure device
3. **Enable MFA** on all accounts if not already enabled
4. **Report exactly what information was disclosed:**
    - Username and password
    - Security questions and answers
    - Personal information (SSN, date of birth, etc.)
    - Financial information (credit card, bank account)
    - Any other credentials or sensitive data

IT Security Will:

- Immediately disable your compromised account
- Monitor for unauthorized access attempts
- Assess risk to other systems and data
- Notify appropriate stakeholders (Legal, HR, affected parties if necessary)
- Guide you through account recovery and security hardening

8.5 Data Breach Response

8.5.1 Suspected Data Breach

If you suspect that Company data has been compromised, lost, or accessed by unauthorized individuals:

1. **Report immediately** to IT Security (within 1 hour)
2. **Do not attempt to assess the scope yourself**
3. **Preserve all evidence** (do not delete emails, logs, or files)
4. **Document what happened:**
    - What data was involved (classification level)
    - How the breach may have occurred
    - When you discovered it
    - Who may have been affected
    - What actions you have taken so far

8.5.2 Data Breach Investigation Process

Upon receiving a data breach report, the Incident Response Team will:

1. **Immediate Response (0-2 hours):**
    - Activate incident response team
    - Contain the breach (isolate affected systems, revoke access)
    - Assess severity and classify incident
2. **Investigation (2-24 hours):**
    - Determine scope of data compromised
    - Identify root cause
    - Assess impact and risk
    - Preserve forensic evidence
3. **Notification (24-72 hours):**
    - Notify senior management and legal counsel
    - Determine regulatory notification obligations (GDPR, PDPA, etc.)
    - Prepare communications for affected individuals

4. **Remediation (Ongoing):**

    - Implement fixes to prevent recurrence
    - Conduct lessons-learned review
    - Update policies and procedures
    - Provide additional training if necessary

8.6 Malware and Ransomware Response

8.6.1 If You Suspect Malware Infection

Indicators of Malware:

- Unusual system slowness or crashes
- Unexpected pop-up windows
- Programs opening or closing automatically
- Unknown programs appearing in startup
- Antivirus alerts or disabled antivirus
- Files encrypted or inaccessible
- Ransom notes or payment demands

Immediate Actions:

1. **Disconnect from network immediately** (unplug Ethernet or disable Wi-Fi)
2. **Do NOT shut down the computer** (unless instructed by IT Security)
3. **Call IT Security immediately:** [Security Hotline]
4. **Do not attempt to remove malware yourself**
5. **Do not pay any ransom** without consulting IT Security and senior management
6. **Take photos** of any ransom notes or error messages (using your phone)

8.6.2 Ransomware Specific Response

If you receive a ransomware notice:

- **Do NOT pay the ransom** without approval from CISO and Legal
- **Isolate the infected system** immediately
- **Do NOT connect external drives** or USB devices
- **Alert IT Security immediately** - ransomware can spread rapidly
- **Preserve the infected system** for forensic analysis
- The Company maintains offline backups; IT will work to restore data

8.7 Incident Response Roles and Responsibilities

8.7.1 All Employees

- Recognize and report security incidents promptly
- Cooperate fully with incident investigations
- Follow instructions from IT Security during incidents
- Maintain confidentiality about ongoing investigations
- Participate in post-incident reviews and training

8.7.2 IT Security Team

- Receive and triage incident reports
- Contain and investigate incidents
- Preserve evidence for analysis
- Coordinate incident response activities
- Communicate with stakeholders
- Document incidents and lessons learned

8.7.3 Incident Response Team

- **CISO:** Overall incident response leadership, strategic decisions
- **IT Director:** Technical response coordination, resource allocation
- **Legal Counsel:** Legal compliance, regulatory notification, liability assessment
- **HR Director:** Employee-related incidents, disciplinary actions
- **Communications/PR:** External communications, media relations
- **Business Unit Leaders:** Business impact assessment, business continuity

8.7.4 Managers

- Support employees in reporting incidents
- Ensure employees are aware of reporting procedures
- Facilitate incident response activities in their teams
- Participate in incident reviews and implement corrective actions

8.8 Post-Incident Activities

After an incident is resolved:

1. **Incident Documentation:** Complete detailed incident report in security incident management system
2. **Lessons Learned Review:** Conduct review meeting with incident response team and affected parties
3. **Root Cause Analysis:** Identify underlying causes and contributing factors
4. **Corrective Actions:** Implement improvements to prevent recurrence
5. **Policy and Procedure Updates:** Revise policies based on lessons learned

6. **Training and Awareness:** Provide additional training to prevent similar incidents
7. **Follow-up:** Verify corrective actions are effective after implementation

9. Compliance and Enforcement

9.1 Compliance Requirements

This policy is mandatory for all individuals with access to Company IT resources. Compliance is monitored through:

- Automated security monitoring and alerting
- Regular security audits and assessments
- Access reviews and recertifications
- Incident reports and investigations
- Security awareness assessments
- Vulnerability scanning and penetration testing

9.2 Consequences of Non-Compliance

Violations of this policy will be taken seriously and may result in:

Violation Severity	Potential Consequences
Minor Violations (unintentional, first offense, low risk)	• Verbal warning • Mandatory security awareness training • Written counseling • Closer monitoring
Moderate Violations (negligent, repeat offense, moderate risk)	• Written warning placed in employee file • Suspension of system access privileges • Performance improvement plan • Suspension without pay (1-5 days)
Serious Violations (intentional, high risk, data exposure)	• Suspension without pay (5-30 days) • Demotion or transfer • Mandatory retraining and probation • Final written warning
Severe Violations (malicious, criminal, extreme risk)	• Immediate termination of employment • Revocation of access to all systems • Referral to law enforcement • Civil litigation for damages • Criminal prosecution

Examples of Severe Violations:

- Installing P2P or Tor software
- Intentional data theft or sabotage
- Fraud or embezzlement using IT systems
- Intentionally spreading malware
- Hacking or unauthorized access to systems
- Sharing access credentials with external parties
- Disabling security controls to facilitate policy violations

9.3 Investigation Process

When a policy violation is suspected:

1. **Initial Assessment:** IT Security reviews the incident and available evidence
2. **Notification:** Employee's manager and HR are notified
3. **Investigation:** Formal investigation conducted by IT Security, HR, and/or Legal
4. **Employee Interview:** Employee given opportunity to provide explanation
5. **Determination:** Decision made regarding policy violation and appropriate consequences
6. **Disciplinary Action:** Consequences implemented according to severity
7. **Appeal:** Employee may appeal decision according to HR grievance procedures

9.4 Reporting Violations

Employees who become aware of policy violations by others should:

- Report violations to IT Security, their manager, or HR
- Not attempt to investigate or confront the violator themselves
- Maintain confidentiality about the report and investigation
- Cooperate with investigations if asked

The Company prohibits retaliation against employees who report policy violations in good faith.

10. Policy Review and Updates

10.1 Regular Review

This policy will be reviewed and updated:

- **Annually** at minimum
- **As needed** in response to:
    - Significant security incidents
    - Changes in technology or threat landscape
    - New legal or regulatory requirements
    - Organizational changes
    - Feedback from employees and stakeholders

10.2 Policy Change Management

- All policy changes will be reviewed and approved by the CISO
- Significant changes require approval from executive leadership
- All changes will be communicated to affected personnel
- Training will be provided on major policy updates
- Version history will be maintained

10.3 Policy Distribution

This policy will be:

- Published on the Company intranet
- Provided to all new employees during onboarding
- Acknowledged annually by all employees (electronic signature required)
- Made available in multiple languages if needed
- Referenced in employment contracts and contractor agreements

Acknowledgment and Acceptance

I acknowledge that:

1. I have received, read, and understood the Global IT Security & Data Privacy Policy
2. I agree to comply with all requirements outlined in this policy
3. I understand that violation of this policy may result in disciplinary action up to and including termination of employment and potential legal action
4. I understand that the Company reserves the right to monitor my use of IT resources
5. I understand that I have no expectation of privacy when using Company IT resources
6. I will report security incidents promptly and cooperate fully with investigations
7. I will complete all required security awareness training

Employee Name: _____

Employee ID: _____

Signature: _____

Date: _____

Approved By:

Chief Information Security Officer (CISO)

Signature: _____

Date: _____

Document Control:

- **Document ID:** SEC-POL-001
- **Version:** 2.0
- **Effective Date:** January 1, 2024
- **Next Review Date:** January 1, 2025
- **Document Owner:** Chief Information Security Officer (CISO)
- **Classification:** INTERNAL

For questions or clarifications regarding this policy, please contact:

IT Security Department

- Email: security@company.com
- Phone: [Security Hotline]
- Service Desk: [Ticket System URL]

END OF POLICY DOCUMENT