Cybersecurity Handbook – ***.com.

Version Control

Version: X.0
Last Updated: [Jan. 1, 2025]
Maintainer: IT Security Team
Reviewed: Bi-annually or after major incidents.

Table of Contents

Onboarding Checklist

All new hires and freelancers must complete the following before accessing ***.com systems:

- Complete cybersecurity training
- Enable multi-factor authentication on all tools
- Install approved antivirus and encryption software
- Sign Non-Disclosure Agreement (NDA)
- Get access to secure work platforms (VPN, Notion, GitHub, etc.)
- Review cybersecurity handbook and acknowledge policy

1. Purpose

This policy outlines mandatory cybersecurity practices at ***.com., a fully remote company committed to developing and promoting ethical AI and machine learning solutions. We comply with ISO/IEC 27001 standards to ensure our information security management system is robust, auditable, and aligned with global best practices.

2. Scope

This policy applies to:
- Full-time and part-time employees
- Freelancers and contractors
- Executives and leadership
- Any individual granted access to company systems or data

3. Core Principles

• Zero Trust Model: Never trust, always verify.
• Least Privilege Access: Only the access needed, nothing more.
• Remote-First Security: Assume hostile environments.
• Human Firewall: People are our first line of defense.
• Privacy by Design: Especially relevant to our work with AI.
• ISO 27001 Alignment: Continuous risk assessment, mitigation, and security governance.

4. Mandatory Security Requirements (All Staff)

• Device Security: Encryption, antivirus, screen lock
• MFA: Required on all platforms
• Secure Internet Use: VPNs for public Wi-Fi
• Data Handling: No local downloads without approval
• Tool Use: Only approved platforms
• Incident Reporting: Must be done within 30 minutes

5. Role-Based Responsibilities and Example Scenarios

CEO & COO

Responsibilities:
- Use hardware security keys
- Attend quarterly security briefings
- Personally approve high-risk data transfers

Example: The CEO approves a request to share an early model with a partner, ensuring encryption and access logs are in place.

IT Manager

Responsibilities:
- Manage access controls and asset inventory
- Lead incident response
- Conduct monthly vulnerability scans

Example: IT receives a report of suspicious login attempts and quickly locks the account, initiates a reset, and performs a root cause analysis.

Freelance Writers

Responsibilities:
- Complete security onboarding
- Use company CMS and tools only
- Avoid storing drafts locally

Example: A freelancer uses Notion for draft collaboration and never stores unencrypted files on their personal laptop.

Content Manager

Responsibilities:
- Approve external tools
- Ensure writer workflows are secure
- Check metadata pre-publication

Example: The content manager denies a request to use a new AI grammar tool due to lack of compliance with ISO 27001 data practices.

6. Remote Work-Specific Expectations

• Private workspaces
• Webcam covers

• No device sharing
• Use separate profiles on shared devices

7. AI/ML Security Guidelines

• Access-controlled model development
• No public AI tool uploads
• Ethical and secure review of AI output
• Compliant dataset usage

8. Violations

Policy violations may result in revoked access, contract termination, and legal action.

9. Policy Review

Reviewed bi-annually or after incidents. All updates must be acknowledged by team members.

10. Contact

IT Security Team - security@***.com
Emergency Slack Channel - #security-alerts

11. Platform-Specific Guidelines

Security requirements vary slightly based on the operating system being used. Below are platform-specific recommendations and mandatory configurations for Windows, Linux, and macOS systems.

Windows Guidelines

• Ensure BitLocker is enabled for full-disk encryption.
• Enable Windows Defender and schedule weekly scans.
• Use Windows Hello for biometric login where available.
• Disable administrative privileges on the daily-use account.
• Keep Windows updated through Windows Update (automatic updates recommended).
• Use group policies (GPO) to enforce security settings for corporate machines.

Linux Guidelines

• Use LUKS or eCryptfs for full-disk encryption.
• Regularly update the system using your distro's package manager (e.g., `apt`, `dnf`, `pacman`).
• Use a firewall like UFW or firewalld and ensure it's enabled on startup.
• Disable root login via SSH.
• Only install software from official or vetted repositories.
• Use AppArmor or SELinux for application sandboxing (based on distro).

macOS Guidelines

• Enable FileVault for full-disk encryption.
• Keep system updated via System Preferences > Software Update.
• Use Gatekeeper and only allow App Store or verified apps.
• Enable the built-in firewall and stealth mode.

• Disable automatic login and ensure password-protected screen saver is active.
• Use a standard (non-admin) user account for daily tasks.

12. Mobile OS Guidelines

For those accessing company systems or communications via mobile devices, the following platform-specific practices must be followed:

iOS (iPhone/iPad) Guidelines

• Enable Face ID or Touch ID with a strong passcode.
• Turn on Find My iPhone and enable device encryption.
• Keep iOS updated automatically (Settings > General > Software Update).
• Only install apps from the App Store.
• Disable Siri access when the device is locked.
• Use Apple's built-in VPN configuration when needed.

Android Guidelines

• Use biometric lock and a strong passcode.
• Enable encryption (usually enabled by default on modern devices).
• Use Google Play Protect and only install apps from Play Store.
• Keep your device updated with the latest security patches.
• Avoid rooted devices; they are not permitted for work use.
• Configure a secure VPN app approved by the IT team.

Chromebook Guidelines

• Enable Verified Boot (on by default) to ensure OS integrity.
• Use strong Google Account passwords with MFA.
• Enforce lock screen and idle timeouts.
• Only install extensions from Chrome Web Store with IT approval.
• Keep Chrome OS up-to-date with automatic updates.
• Enable and use Smart Lock or PIN login features for secure access.

13. International Compliance Guidelines

As a globally distributed company, ***.com. is committed to adhering to international cybersecurity and data privacy laws. Employees and contractors must understand and comply with applicable regulations in their jurisdictions and in the jurisdictions where our clients operate.

Key Regulatory Frameworks

• **GDPR (EU/EEA)** – General Data Protection Regulation:
  - Requires lawful basis for processing personal data.
  - Data subjects have rights to access, rectify, and erase data.
  - Breach notification must occur within 72 hours.

• **CCPA/CPRA (California, USA)** – California Consumer Privacy Act:
  - Right to know, delete, and opt out of data selling.
  - Transparency required about data collection practices.

• **PIPEDA (Canada)** – Personal Information Protection and Electronic Documents Act:
  - Requires knowledge and consent for data collection.
  - Businesses must protect personal information using appropriate safeguards.

• **LGPD (Brazil)** – Lei Geral de Proteção de Dados:
  - Similar to GDPR with a focus on transparency and user consent.

• **ISO/IEC 27001** – International Standard:
  - Focuses on establishing, implementing, maintaining, and continually improving an information security management system (ISMS).
  - ***.com follows ISO/IEC 27001 for global cybersecurity alignment.

Responsibilities of Team Members

• Understand your local data protection laws.
• Report cross-border data transfers to IT and legal.
• Use only approved tools that comply with international regulations.
• Follow privacy-by-design principles when developing features, writing content, or processing any user or client data.
• Complete all mandatory compliance training during onboarding and annually thereafter.

14. Glossary of Key Terms

MFA – Multi-Factor Authentication – A method of confirming a user's identity using two or more verification methods.

VPN – Virtual Private Network – A secure tunnel that encrypts data between your device and the internet.

Zero Trust – A security model where no user or device is trusted by default, even inside the network.

Encryption – The process of converting information into a secure format so unauthorized parties cannot access it.

ISO/IEC 27001 – An international standard for managing information security.

Phishing – A type of cyberattack where attackers trick users into revealing personal information.

Firewall – A network security system that monitors and controls incoming and outgoing traffic.

15. Tool Configuration Guidelines

The following are standard configurations for tools approved at ***.com:

• **Google Workspace**
  - MFA required on all accounts
  - Sharing restricted to company domain only

• **Slack**

- Channels for work only, no external integrations without approval
- Use #security-alerts for incident reports

• **GitHub**
- Use SSH keys, not passwords
- Private repositories only unless otherwise cleared

• **Notion**
- Workspace access via company email only
- Role-based permissions enforced

• **VPN (e.g., NordLayer)**
- Always-on VPN for anyone accessing client or internal systems
- Only connect from approved devices

16. Appendix: Security Templates

Incident Response Report Template

Incident Title:
Date/Time Detected:
Detected By:
Description:
Systems Affected:
Immediate Actions Taken:
Root Cause Analysis:
Resolution Date:
Follow-up Recommendations:

Data Breach Notification Template

Subject: Security Breach Notification

To Whom It May Concern,

We are writing to inform you that a data breach was detected on [Date]. Our investigation determined that [summary of breach]. Data potentially affected includes [types of data].

We have taken immediate action to contain the breach and are cooperating with relevant authorities. We encourage you to [recommended action].

For further assistance, contact [contact person/email].

Sincerely,

[Your name]
***.com