Acceptable Use Policy

Background

[Company Name] is committed to ensuring all workforce members actively address security and compliance in their roles at [Company Name]. We encourage self-management and reward the right behaviors.

Purpose

This policy specifies the acceptable use of end-user computing devices and technology. Additionally, training is imperative to assure an understanding of current best practices, the different types and sensitivities of data, and the sanctions associated with non-compliance.

Roles and Responsibilities

This policy is owned by Legal and Security. Legal and Security will coordinate with the People and Information Technology departments as needed for administration of this policy.

Policy

[Company Name] policy requires all workforce members to comply with the Acceptable Use Policy. [Company Name] policy requires that:

- Background verification checks on all candidates for employees and contractors should be carried out in accordance with relevant laws, regulations, and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risk.
- Employees, contractors, and third-party users must agree to and sign the terms and conditions of their employment contract, and comply with acceptable use.
- Employees will go through an onboarding process that familiarizes them with the environments, systems, security requirements, and procedures [Company Name] has in place. Employees will also have ongoing security awareness training that is audited.
- Employee off-boarding will include reiterating any duties and responsibilities still valid after terminations, verifying that access to any [Company Name] systems has been removed, as well as ensuring that all company-owned assets are returned.
- [Company Name] and its employees will take reasonable measures to ensure no corporate data is transmitted via digital communications such as email or posted on social media outlets.
- [Company Name] will maintain a list of prohibited activities that will be part of onboarding procedures and have training available if/when the list of those activities changes.

- A fair disciplinary process will be utilized for employees that are suspected of committing breaches of security. Multiple factors will be considered when deciding the response, such as whether or not this was a first offense, training, business contracts, etc. [Company Name] reserves the right to terminate employees in the case of serious cases of misconduct.

Procedures

[Company Name] requires all workforce members to comply with the following acceptable use requirements and procedures, such that:

- All workforce members must follow all system access controls and procedures for information access.
- Use of [Company Name] computing systems and SaaS applications are subject to monitoring by [Company Name] IT and/or Security teams.
- Employees may not leave computing devices (including laptops and smart devices) used for business purposes, including company-provided and BYOD devices, unattended in public.
- Device encryption must be enabled for all mobile devices accessing company data, such as whole-disk encryption for all laptops.
- All email messages containing sensitive or confidential data will be encrypted.
- Employees may not post any sensitive or confidential data in public forums or chat rooms. If a posting is needed to obtain technical support, data must be sanitized to remove any sensitive or confidential information prior to posting.
- All data storage devices and media must be managed according to the [Company Name] Data Classification specifications and Data Handling procedures.

Protection Against Malware

[Company Name] protects against malware through malware detection and repair software, information security awareness, and appropriate system access and change management controls. This includes:

- Anti-malware or equivalent protection and monitoring must be installed and enabled on all endpoint systems that may be affected by malware, including workstations and laptops. Regular scans will include:
    - Any files received over networks or via any form of storage medium, for malware before use;
    - Electronic mail attachments and downloads for malware before use; this scan should be carried out at different places, e.g. at electronic mail servers, desktop computers, and when entering the network of the organization;
    - Web pages for malware.
- Restrictions on Software Installation

    - Only legal, approved software with a valid license installed through a pre-approved application store will be used. Use of personal software for business purposes and vice versa is prohibited.
    - The principle of least privilege will be applied, where only users who have been granted certain privileges may install the software.
    - [Company Name] will identify what types of software installations are permitted or prohibited.
- Vulnerabilities that could be exploited by malware will be reduced, e.g. through technical vulnerability management.
- [Company Name] will conduct regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated.
- Malware detection and repair software will be installed and regularly updated to scan computers and media as a precautionary control, or on a routine basis; the scan carried out will include:
    - Any files received over networks or via any form of storage medium, for malware before use;
    - Electronic mail attachments and downloads for malware before use;
- Defining procedures and responsibilities to deal with malware protection on systems, training in their use, reporting, and recovering from malware attacks.
- Preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements.
- Implementing procedures to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware.
- Implementing procedures to verify information relating to malware, and ensure that warning bulletins are accurate and informative; managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites, or suppliers producing software protecting against malware, are used to differentiate between hoaxes and real malware; all users should be made aware of the problem of hoaxes and what to do on receipt of them.
- Isolating environments where catastrophic impacts may result.

Protection Against Exposure of Data

[Company Name] protects against the exposure of data while using ChatGPT and similar conversation artificial intelligence (AI) technologies by users agreeing to adhere to the below acceptable use guidelines. These guidelines are essential for safeguarding confidential information and maintaining the integrity of business operations. Failure to adhere to these guidelines may result in the termination of your access to the service.

- Only authorized personnel who have a legitimate need for using the service may use ChatGPT or similar technologies. This is to minimize the risk of unauthorized exposure of business data.

- Do not share, transmit, or request any confidential or sensitive business data through ChatGPT or similar technologies. This includes, but is not limited to, financial information, trade secrets, customer data, intellectual property, and any proprietary or classified information.

Revision History