Acceptable Use Policy

ENTITY

Purpose

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

Scope

- Applies to all ENTITY personnel who utilize company IT assets.
- Company assets are those assets that are owned or managed by ENTITY.

ENTITY 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 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 ENTITY has in place. Employees will also have ongoing security awareness training that is audited.
- Employee offboarding will include reiterating any duties and responsibilities still valid after terminations, verifying that access to any ENTITY systems has been removed, as well as ensuring that all company owned assets are returned.
- ENTITY 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.
- ENTITY 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. ENTITY reserves the right to terminate employees in the case of serious cases of misconduct.

Procedures

ENTITY requires all workforce members to comply with the following acceptable use requirements and procedures, such that:

- All workforce members are primarily considered as remote users and therefore must follow all system access controls and procedures for remote access.
- Use of ENTITY computing systems is subject to monitoring by ENTITY 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 ENTITY Data Classification specifications and Data Handling procedures.
- Employees may only use photocopiers and other reproduction technology for authorized use.
- Media containing sensitive/classified information should be removed from printers immediately.
- The PIN code function will be used on printers with such capability, so that the originators are the only ones who can get their print-outs and only when physically present at the printer.

Protection Against Malware

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

- 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 software.
    - ENTITY will identify what types of software installations are permitted or prohibited.
- Anti-malware or equivalent protection and monitoring must be installed and enabled on all endpoint systems that may be affected by malware, including workstations, laptops and servers.

- Controls that prevent or detect the use of unauthorized software (e.g. application allowlisting) will be implemented.
- Controls that prevent or detect the use of known or suspected malicious websites (e.g. blocklisting) will be implemented.
- Vulnerabilities that could be exploited by malware will be reduced, e.g. through technical vulnerability management.
- ENTITY 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; 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.
- ENTITY will determine the defense principles, effective placement, and configuration of malware detection and repair tools based on risk assessment outcomes; considerations will include:
    - Evasive techniques of attackers (e.g. the use of encrypted files) to deliver malware or the use of encryption protocols to transmit malware;
    - Protection against the introduction of malware during maintenance and emergency procedures, which can bypass normal controls against malware;
    - Implementing a process to authorize temporarily or permanently disable some or all measures against malware, including exception approval authorities, documented justification and review date.
- 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.
- Where possible, disable USB ports, prohibit writable media use, and restrict read-only media to legitimate commercial sources and allowlisted software.