# Information Security Standard – Rules of Behavior

## Policy Statement

This Standard supports the {Company} Information Security & Privacy Policy and outlines the rules of behavior for the use of and access to {Company}’s systems and information assets.

### Applicability

Compliance with the rules outlined in this document is mandatory for all {Company} employees, contractors, vendors, and any others with access to {Company}’s systems or information assets.

### Non-compliance

Any instances of non-compliance with the controls outlined in this document should be reported following the procedures outlined in the Reporting Process.

### Scope

The requirements of this standard apply to all systems that store, process, or transmit {Company} information; or are used to connect to those systems that are used to store, process, or transmit {Company}’s information.

## Rules of Behavior

### Users shall:

* Prevent unauthorized disclosure or modification of sensitive information.
* Immediately report
  + all lost or stolen {Company} equipment,
  + known or suspected security incidents,
  + known or suspected information security policy violations or compromises,
  + any other suspicious activity.

This includes an actual or potential loss of control or compromise - intentional or not - of authenticator, password, or other sensitive information, including Personally Identifiable Information (PII), maintained by or in the possession of {Company}.

* Ensure that software, including downloaded software, is properly licensed and free of malicious code before installing and using it on {Company} systems.
* Ensure that all third-party software incorporated into the {Company} platform is tracked and logged.
* Log-off or lock systems when leaving them unattended.
* Use appropriate access restrictions and unique accounts to access information.
* Avoid sharing accounts whenever possible, and only share credentials by secure means. Individual accounts should never be shared.
* Complete security awareness training before accessing any {Company} system and on an annual basis thereafter; as well as complete any specialized role-based security or privacy training as required. Security training materials and supporting documentation for {Company}’s Information Security Program can be found here.
* Permit only authorized {Company} users to use {Company} equipment and systems.
* Secure sensitive information when not immediately in use.
* Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed.
* Only access sensitive information necessary to perform job functions (least privilege).
* Use PII, ePHI, PCI, or other sensitive information only for the purposes for which it was collected, to include conditions set forth by {Company}’s Privacy Policy, Acceptable Use Policy, and Terms of Service.

### Users shall not:

* Direct or encourage others to violate {Company} policies.
* Circumvent security safeguards or reconfigure systems except as authorized (i.e., violate least privilege).
* Use another person’s account, identifier, or password.
* Remove computers or equipment without authorization.
* Send or post threatening, harassing, intimidating, or abusive material about others in public or private messages or forums.
* Exceed authorized access to sensitive information.
* Store sensitive information in public folders or other insecure physical or electronic storage locations.
* Share sensitive information, except as authorized and with formal agreements that ensure third parties will adequately protect it. This includes the posting of information on social media sites.
* Transport, transfer, email, remotely access, or download sensitive information; unless such action is explicitly permitted by the manager or owner of such information.
* Store sensitive information on portable devices such as laptops and USB drives or on remote/home systems without authorization or appropriate safeguards.
* Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for self or others.
* Copy or distribute intellectual property — including music, software, documentation, and other copyrighted materials — without permission or license from the copyright owner.

### Users shall ensure the following protections are properly engaged, including on non-{Company} equipment or equipment housed outside of {Company} facilities:

* Use anti-malware software and firewalls configured to automatically update.
* Provide adequate physical controls for areas and systems containing sensitive information.
* Use approved encryption to protect sensitive information stored on portable devices or recordable media, including laptops, thumb drives, and external disks; stored on remote or home systems; or transmitted or downloaded via e-mail or remote connections.
* Use two-factor authentication for remote access to sensitive information.

### Users shall ensure that passwords:

* Are at least 12 characters in length
* Have sufficient entropy and complexity to prevent easy cracking
* Are changed in the event of known or suspected compromise, and immediately upon system installation (e.g., default or vendor-supplied passwords are never allowed)
* Are not reused across systems or sites
* Are committed to memory, or stored in a secure manner
* Are only shared with other employees via LastPass or other manner approved by the Head of Security.

### Signature

I have read the {Company} Rules of Behavior and understand and agree to comply with its provisions. I understand that violations of the {Company} Rules of Behavior or Information Security Policy and Supporting Standards may lead to disciplinary action, up to and including termination of employment, as well as civil and criminal penalties. I also understand that violation of laws and regulations that pertain to {Company}’s Information Systems can result in monetary fines and/or criminal charges that may result in imprisonment; and that I am solely liable for any such violations.

## Appendices

### Document Management

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Syltor Consulting | Version | 1.1 |
| Date Modified | 30 May 2019 | Approver |  |
| Last Reviewed |  | Reviewer(s) |  |
| Review Cycle | Annual | Next Review Date |  |