**COMPANY Logo**

**Information Security Policies:** Personnel Management

Effective Date:

**COMPANY Logo**

Revised:

Approved by: CISO Approved on: 00/00/20XX

Approved by: COO Approved on: 00/00/20XX

Approved by: Board of Directors Approved on: 00/00/20XX

# Purpose

The purpose of the Personnel Management Policy is to ensure that Users (employees, contractors, vendors, consultants, or other persons) who work with COMPANY (“COMPANY”) understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of COMPANY resources.

# Scope

This policy applies to Users having access to COMPANY computing assets or information. It applies to all systems used to conduct COMPANY business, and applies to internal COMPANY information and information shared with and received from third parties. It covers security responsibilities that should be addressed prior to employment, during employment, and at termination.

# Roles and Responsibilities

## The RACI Chart below shows the assignment of functional and cross-functional activities. The roles are as follows:

| R - Responsible is the organizational title responsible for doing the work.A - Accountable is the organizational title for who is accountable for the work being done.C - Consulted is the organizational title that provides necessary information.I - Informed is the organizational title that receives information. **Milestone or Task** | Governance / Risk Management | Chief Information Security Officer | Information Security Organization / IT | HR Manager | Users |
| --- | --- | --- | --- | --- | --- |
| Personnel Practices | C | A | I | R | R |
| Acceptable Use | C | A | R | I | R |
| Security Awareness & Training | C | A | R | I | R |
| Termination | C | A | R | R | I |

# Policy Statements

The Personnel Management Policy is implemented because there are three aspects to information security: people, process, and technology. It is important to ensure that security is an integral part of all personnel focused guidelines.

This is accomplished via the following:

## Personnel Practices

* + 1. Human Resources must ensure that job descriptions clearly define security responsibilities. At a minimum, they must ensure all users understand that they must comply with Information Security Policies.
    2. Human Resources must include a full job description in Employment contracts.
    3. Human Resources must describe generic security responsibilities in Employment contracts.
    4. Human Resources must provide specific guidance on security responsibilities in Employment contracts.
    5. Human Resources must include a statement of compliance with applicable laws and regulations in Employment contracts.
    6. Human Resources must include a statement of compliance with Information Security Policies in Employment contracts.
    7. Human Resources must identify acceptable use of COMPANY information and information resources in Employment contracts.
    8. Human Resources must state in the Employee Manual the importance of and compliance with Information Security Policies.
    9. Human Resources must include a section on security, Information Security Policies, information classification, and data protection in all performance reviews.
    10. Human Resources must perform a thorough background check on all personnel to be placed in business or computer related positions of trust. A thorough background check includes the following:

• Reference check (verbal or written)

• Identity check

• Academic qualifications check

• Employment history check

• Criminal record check

• Credit check

* + 1. Human Resources must ensure that each user understands the disciplinary actions that will take place upon non-compliance with Information Security Policies. Intentional non-compliance with Information Security Policies is grounds for disciplinary action including termination.
    2. Users must be accountable for understanding their security responsibilities.
    3. Users must sign a statement that acknowledges they understand and intend to abide by security policies.
    4. Users must sign a Confidential Disclosure Agreement (CDA) prior to gaining access to any information and information technology (IT) asset.

## Acceptable Use

* + 1. The Information Security Organization must ensure Internet access is monitored, controlled, and secured.
    2. The Information Security Organization must ensure all commercial software, upgrades, and patches downloaded from remote, non-COMPANY sources are tested on a standalone PC before being loaded onto the network.
    3. The Information Security Organization must ensure that all email attachments, regardless of the source or content, are scanned for viruses and other destructive programs before being opened, or stored on any business computer system.
    4. The Information Security Organization must ensure that any material that is transmitted to other users via email must be scanned for viruses before it is sent.
    5. Users must understand the acceptable uses of information, information resources, the Internet, and email information and computer resources.
    6. Users must use COMPANY equipment for business, business related, and employee personal use (only when personal use is of an incidental nature and does not interfere with business activities). This includes non-business related communications containing puzzles, games, pictures, video / sound files, and large file attachments.
    7. Users must conduct activities on the Internet and email with the reputation of COMPANY in mind. Users must remember that when they visit remote sites or send emails they are viewed as representatives of COMPANY, and accordingly must adhere to the highest standards of conduct. Users must exercise the same care in sending emails, communicating in chat groups, and posting items to newsgroups as they would for any other written communication that bears the corporate logo.
    8. Users must not create or participate in blogs or chat rooms that deal with COMPANY, its employees, customers, or its business.
    9. Users must not create or distribute electronic communications containing copyrighted materials without appropriate authorization and consent from the author or publisher.
    10. Users must not send external communications containing Non-Public Information including Social Security Numbers.
    11. Users must waive all rights to privacy in anything they create, store, send, or receive on COMPANY computer systems or the Internet. COMPANY reserves the right to monitor any and all aspects of its information system and network to ensure compliance with COMPANY *Access Controls Management Policies*. Monitoring includes, but is not limited to, tracking the sites the users visit on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded.
    12. Users must understand there is no assumption of privacy with respect to email. Although COMPANY does not routinely monitor email messages, email must be subject to archival policies and as such, could be subject to the same scrutiny normally afforded to paper files and documents. COMPANY reserves the right to access these systems without notice. Users must not assume that any information, including messages or data that have been "deleted" is private.
    13. Users may incur criminal or civil liability for actions that violate systems or network security. COMPANY will cooperate fully with investigations of violations of systems or network security at other sites, including cooperating with law enforcement authorities in the investigation of suspected criminal violations.
    14. Users must not use COMPANY resources for prohibited activities including, but are not limited to the following:

• Unauthorized use of COMPANY resources.

• Exceeding the scope of authorized access into computers.

• Altering, modifying or destroying files or data of others without the explicit consent of the system, asset, or program owner.

• The introduction of software or hardware into any computer system that is intended to disrupt normal operations. This includes programs known to carry a destructive or non-destructive "virus", "worm", "logic bomb", or "Trojan Horse". In addition to violating COMPANY ethics standards, such actions may be illegal, and punishable by state and federal law.

• Circumvention, or attempting to circumvent, security measures of any host, network, or account ("cracking"). This includes, but is not limited to, accessing data not intended for the User, logging into a server or account the User is not authorized to access.

• Probing the security of any COMPANY computer or network is restricted to specifically authorized members of IT with engagement rules specified and agreed to in advance by the CISO (or equivalent). The use of "sniffing" software or hardware, or probing tools such as SATAN may be allowed for such engagements. Any security probing by users is expressly prohibited.

• Attempting to interfere with service to any user, host, or network ("denial of service attacks"). This includes, but is not limited to; "flooding" of networks, deliberate attempts to overload a service, and attempts to "crash" a host.

• Trafficking in, or facilitating in the trafficking in unauthorized, counterfeit, or fraudulently obtained passwords, access codes, “cracker” software, or other access devices

• Unnecessary web browsing.

• Engaging in conduct that is harassing, threatening, or a sexual advance.

• Engaging in “flame” wars.

• Using COMPANY equipment or facilities to develop or use programs that infiltrate or attempt to infiltrate a computer or computing system and/or damage or alter the software components of a local or remote computer or computing system.

* + 1. Users must not use COMPANY resources for commercial or personal advertisements.
    2. Users must not use COMPANY resources for solicitations or promotions of any outside business.
    3. Users must not use COMPANY resources for political lobbying or promoting political activities.
    4. Users must not use COMPANY resources for any commercial purpose other than official COMPANY business
    5. Users must not use COMPANY resources to engage in actions that violate trademark laws.
    6. Users must not use COMPANY resources to view or distribute pornography, child pornography, or obscene materials, photographs or files.
    7. When using COMPANY Information assets Users must not use COMPANY resources for the transmission, distribution, or storage of any information, data or material in violation of United States or state regulation or law, or by the common law, is prohibited. This includes, but is not limited to, material protected by copyright, trademark, trade secret, or any other statute.
    8. Users must access the Internet via an approved Internet connection that passes through a COMPANY authorized firewall or web filtering proxy.
    9. Users must only access the Internet by modem when approved in specific circumstances, and only if the accessing computer is not simultaneously connected to the business network.
    10. Users must not download software, freeware, and shareware.
    11. Users must not download commercial software, upgrades, and patches.
    12. Users must not be allowed to perform Anonymous FTP uploads or downloads.
    13. Users must use disclaimers such as "These statements are solely my opinion, and do not necessarily reflect the views of my employer." when any statements or comments are posted to newsgroups and the like that are not official COMPANY statements.
    14. When using COMPANY Information assets users must not contact sites that are inappropriate to contact through COMPANY facilities and equipment. Examples of such sites may include but are not limited to:

• Sexually explicit sites

• Hacker sites

• warez or pirated software related sites

• Sites that may conflict with COMPANY policies and/or business interests

While a rare, singular connection to such a site could occur due to a misleading or inaccurate link, any repetitive access would be construed as a serious violation of corporate policy.

* + 1. Users must not use re-mailer services, drop-boxes, or identity stripping.
    2. Users must not use the Internet for playing games.
    3. Users must not use Internet access for sending or retrieving pornographic material, inappropriate text files, or files dangerous to the integrity of the network.
    4. Users must not use the Internet in ways that violate federal, state, or local laws or statutes.
    5. Users must use only their own COMPANY allocated email account. Each user is responsible for all email sent from their COMPANY account. COMPANY will assume that any email message sent from a user’s account originated from that user.
    6. Users must exercise the same care in drafting email as they would for any other written communication that bears the corporate logo.
    7. Users must not obligate legal or contractual agreements for COMPANY through email.
    8. Users must use a disclaimer such as "These statements are solely my opinion, and do not necessarily reflect the views of my employer" and other necessary or required disclosures approved by the Compliance Department; for any statements or comments made via email that could in any way be construed as a COMPANY action.
    9. Users must not send messages that contain any material that may reasonably be considered offensive, disruptive, defamatory, or disparaging towards any employee or COMPANY. Offensive content includes, but is not limited to,

• Sexual comments or images

• Racial or religious slurs

• Gender specific comments

• Workplace gossip

• Disparagement of the firm, co-workers, vendors, or customers

* + 1. Users must not publish or distribute internal mailing lists to non-employees.
    2. Users must not execute any programs (excluding ZIP, WAVE, avi, wmv, mp3 JPEG, Word Macros, and similar) that are received via e mail.
    3. Users must not install any upgrades or patches received via e mail.
    4. Users must not forward or otherwise propagate chain letters, ponzi schemes, or pyramid schemes to lists or individuals, and any other types of use, which may unnecessarily consume system resources or otherwise interfere with the work of others.
    5. Users must not send unsolicited bulk mail messages ("junk mail" or "spam"). This includes, but is not limited to, bulk-mailing of commercial advertising, informational announcements, and political tracts.
    6. Users must not send malicious email, including but not limited to "mailbombing" (flooding a user or site with very large or numerous pieces of email).
    7. Users must not post network or server configuration information about any COMPANY machines. This includes internal tcp addresses, server names, server types, or software version numbers.
    8. Users must identify themselves by their real name; pseudonyms that are not readily attributable to actual users are not allowed. Users must not represent themselves as another user.
    9. Users must not forge header information.
    10. Users must not use any external Web mail services (such as AOL, Hotmail, Yahoo, Google, etc.) on COMPANY’s computer systems.
    11. Networking web sites that are designed primarily to be used for electronic communications among users are not permitted at this time as the firm does not currently have the technology or systems to monitor or retain those communications.
    12. User must identify the company name, contain full disclosure, provide no false or misleading information, and not present any forward-looking statements for all postings to any networking web site.
    13. Users must not use a networking web site for personal use during business hours. Using the firm’s computer systems to access networking web sites other than LinkedIn is prohibited. Any personal bio an employee includes on her or his personal site, which includes reference to the firm, should limit the information about the firm to the firm’s name.
    14. Users must not copy or transmit to any outside party any software that has been installed on COMPANY computers.

## Security Awareness and Training

* + 1. The Information Security Organization must make new users aware of the security policies and data classification as part of their orientation and existing users must periodically receive information security awareness training.
    2. Users must periodically receive information security awareness briefings, such as “Security 101” or general security, refreshers to the security policies and data classification, and other security awareness briefings as necessary.
    3. Users must be made aware of the information ethics that addresses the protection, use, duplication, sharing or disclosure of COMPANY information.
    4. Users must receive security training specific to their job functions such as network and system security and also secure software development for application developers.
    5. Users must sign an Information Security Policies Acknowledgment form. This form will acknowledge that each new user has read the Information Security Policies and understands the responsibilities concerning the policies and the consequences of a policy infraction.

## Termination

* + 1. The Information Security Organization must maintain formal procedures to terminate information access privileges for users. The resigning individual’s manager must notify Human Resources (HR) immediately when an employee, contractor, or consultant leaves COMPANY. HR will then immediately notify IT who will implement procedures for resignations based upon the resigning individual’s access to sensitive information. The administrators on the appropriate systems will remove the resigning individual’s user ID(s).
    2. The Information Security Organization must ensure that all property, including all computer equipment, in the custody of the user is returned.
    3. The Information Security Organization must ensure all system access cards are retrieved prior to departure and such access cards must be deactivated.
    4. The Information Security Organization must ensure all relevant passwords are changed if the resigning user was responsible for system administration.
    5. The Information Security Organization must ensure that various passwords are expired based on the resigning user’s access to sensitive information.
    6. The Information Security Organization must ensure that all information from user-owned equipment, including equipment in a user’s home is erased.
    7. The Information Security Organization must maintain formal procedures to remove involuntarily terminated individuals from COMPANY premises. The terminated individual’s manager must notify HR when an employee or contractor is being involuntarily terminated. HR will then immediately notify IT who will implement procedures for involuntarily termination based upon the terminated individual’s access to sensitive information. The administrators on the appropriate systems will remove the terminated employee’s user ID(s). All user ID(s) must be removed prior to employee notification of termination.

# Compliance with Policies

# Use of COMPANY’s network, systems, hardware and applications represents the User’s consent to the terms of the policies described here, including consent for COMPANY to monitor and audit content and/or use. A User’s failure to comply with Information Security Policies may lead to disciplinary action to include one or more of the following:

* Oral and/or written warning or notification of violation to User(s) involved and supervisor(s)
* Suspension of network, system or application access or electronic communications privileges permanently or for a set period
* Repossession of electronic devices or hardware permanently or for a set period
* Electronic messages may be blocked or rejected if the message contains inappropriate content
* Written warning to the User’s HR file
* Suspension from work
* Education course related to the infraction paid for by the User
* Regulatory discipline or censure
* Termination of employment

Users consent by reading this policy at time of hiring and at each annual evaluation by signing an *Information Security Policy Acknowledgement* form.

# Questions

Users are encouraged to contact the Chief Information Security Officer (CISO) or the Information Security Organization with any questions or concerns. It is critical for all Users to consult supervisors and/or the Information Security Organization about “red flags” (any suspicious activities giving rise to concerns about whether such activities meet or potentially violate Information Security Policies). All Users are encouraged to raise questions or concerns if they believe an information-security risk or leak is present.

# Disclaimers

COMPANY retains the right to:

* Restrict or revoke any User’s privileges to information, equipment or systems
* Inspect, copy, remove or otherwise alter any information, program, or other system resource that may undermine these objectives
* Take any other steps deemed necessary to protect COMPANY information or information systems

This right may be exercised with or without notice to the involved users. COMPANY disclaims any responsibility for loss or damage to information or software that results from COMPANY exercising its rights under Information Security Policies.

All documents, computing assets, and communications systems assets, including the email and phone systems, physically located at or pertaining to COMPANY are the property of COMPANY. COMPANY reserves the right to examine all information stored in or transmitted by these systems, subject to applicable law. Users should have no expectation of privacy associated with personal information and information stored in, created on, or sent through the COMPANY computer and communication systems.

# Definitions

The following terms are related to this Information Security Policy:

* **Compromise**: Disclosure of data to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, may have occurred.
* **Confidentiality**: The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.
* **Electronic Communications Systems**: All forms of communicating via electronic means such as the Internet, facsimile, cell phone, cable, PDAs, computers, networks, etc.
* **Electronic Messaging**: All forms of communicating such as Email, video conferencing, phone, IM, etc. via electronic means.
* **Email**: The electronic transmission of information through a mail protocol such as SMTP, POP3, or IMAP.
* **Encryption**: The protection of data during storage or transmission by cryptographic means.
* **Forwarded Email**: Email resent from an internal network to an outside point.
* **Information Classification**: The determination that information is sensitive and requires a specific degree of protection against unauthorized disclosure.
* **Information Resources (IR)**: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
* **Information Security**: Includes the concepts, techniques, technical, administrative, and managerial measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, manipulation, modification, loss, or use.
* **Portable Electronic Communications Systems**: Mobile electronic communications systems such as cell phones, Blackberry’s, Iphones, Treos, iPaqs, Palms, PDAs, laptops, netbooks etc..
* **Security Awareness**: An initiative that sets the stage for security by changing organizational attitudes to realize the importance of security and the adverse consequences of security failure. Further, awareness reminds users of the importance of security and the procedures to be followed.
* **Security Policies**: The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive data.
* **Security Training**: The teaching of specific security skills and knowledge, usually directed at a predefined topic area such as network security, Windows security, wireless security, etc.
* **Unauthorized Disclosure**: The intentional or unintentional revealing of restricted information to people both inside and outside the organization, who do not have a “need to know” for that information.