POLICY

Cyber Security

Location:
Effective Date:
Revision Number: 1

TABLE OF CONTENTS

PURPOSE OF THE CYBER SECURITY POLICY

The Cyber Security Policy forms the foundation of the corporate Information Security Program. Information security policies are the principles that direct managerial decision-making and facilitate secure business operations. A concise set of security policies enables the IT team to manage the security of information assets and maintain accountability. These policies provide the security framework upon which all subsequent security efforts will be based. They define the appropriate and authorized behavior for personnel approved to use information assets.

This policy includes three distinct components:

- General Email/Internet Security and Use
- Bring Your Own Device (BYOD) and Acceptable Use
- Online Social Networking

APPLICABILITY

The Cyber Security Policy applies to all employees, interns, contractors, vendors and anyone using assets. Policies are the organizational mechanism used to manage the confidentiality, integrity and availability issues associated with information assets. Information assets are defined as any information system (hardware or software), data, networks, and components owned or leased by or its designated representatives.

GENERAL EMAIL/INTERNET SECURITY AND USE

General Security Policy

All employees, contractors, vendors, and any other person using or accessing information or information systems must adhere to the following policies:

- All information systems within are the property of and will be used in compliance with policy statements.
- Any personal information placed on information system resources becomes the property of .
- Any attempt to circumvent security policy statements and procedures (e.g., disconnecting or tunneling a protocol through a firewall) is strictly prohibited.
- Unauthorized use, destruction, modification and/or distribution of information or information systems is prohibited.
- All users will acknowledge understanding and acceptance by signing the appropriate policy statements prior to use of information assets and information systems.
- At a minimum, all users will be responsible for understanding and complying with the following policy statements:
    - General Security Policy
    - System Security Policy
    - Password System Security
    - Desktop Service Security Policy
    - Internet Acceptable Use Policy
    - Email Security Policy
    - Personal Equipment Policy
    - Virus, Hostile and Malicious Code Policy
- All users will report any irregularities found in information or information systems to the IT team immediately upon detection.
- information systems and information will be subject to monitoring at all times. Use of information systems constitutes acceptance of this monitoring policy.
- Use of any information system or dissemination of information in a manner bringing disrepute, damage or ill will against is not authorized.

- Release of information will be in accordance with policy statements
- Users will not attach their own computer or test equipment to computers or networks without prior approval of the IT team or its designated representative.

System Security Policy

’s System Security Policy addresses access control, use of hardware, operating systems, software, servers and backup requirements for all systems maintained and operated by .

The System Security Policy applies to all employees, contractors, vendors, and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the chief information officer (CIO) or his or her designated representative.

Password System Security

In today’s information age, poorly selected, reusable passwords represent the most vulnerable aspects of information security. has adopted this policy to ensure that the private information of our clients and our proprietary corporate data are kept secure at all times. authorized users must comply with creation, usage and storage policies to minimize risk to corporate information assets:

- Passwords will conform to the following criteria:
    - Passwords will be a minimum of eight characters
    - Passwords must consist of at least one uppercase letter, one lowercase letter and one number.
- The sharing of passwords is prohibited.
- Any suspicious queries regarding passwords will be reported to the IT team.
- Passwords will be protected as proprietary information. Writing them down or storing them unencrypted on the information system is prohibited.
- Users must change their passwords every 90 days and may reuse passwords only after 10 different passwords have been used.
- Accounts will be locked out after five failed password attempts in a 30-minute time period. Accounts can be reset by contacting the IT team or by waiting 30 minutes for the account to reset automatically.
- Users will be forced to unlock their computers using their network password after 60 minutes of inactivity on their desktops.
- All system passwords will be changed within 24 hours after a possible compromise.
- When users leave the organization, their accounts will be immediately disabled or deleted.
- If the user leaving the organization was a privileged user or a network administrator, all system passwords will be changed immediately.

Desktop Services Security Policy

The Desktop Services Security Policy addresses the authorized and legitimate use of hardware, operating systems, software, local area network (LAN), file servers and all other peripherals used to access any information system:

- No software of any kind will be installed onto a laptop or desktop computer without the approval of the IT team.
- Only system administrators will have the ability to install software.
- Unauthorized copying or distributing of copyrighted software is a violation of federal copyright law and will not be permitted.
- Personal software will not be installed on any machine.
- Users will not allow non-employees to use any machine or device without authorization of the IT team.
- The following items are corporate policy for security monitoring:

- All systems and network activities will be subject to monitoring. Use of systems and networks constitutes consent to this monitoring.
- Disabling or interfering with virus protection software is prohibited.
- Disabling or interfering with logging, auditing or monitoring software is prohibited.
- All desktop services will be subject to inventory and inspection.
- Security irregularities, incidents, emergencies and disasters related to information or systems will be reported to the IT team immediately.

- The following items are corporate policy for system usage:
  - Sabotage, destruction, misuse or unauthorized repairs are prohibited on information systems.
- All repairs will be authorized and performed by the IT team:
  - Desktop resources will not be used to compromise, harm, destroy or modify any other service or resource on the information system.
  - All data on information systems at is classified as company proprietary information.
  - Users will secure all printed material and other electronic media associated with their use of information and information systems.
  - Storage, development or the unauthorized use of tools that compromise security (such as password crackers or network sniffers) are prohibited.

Internet Acceptable Use Policy

Internet access is provided to employees to conduct business. While these resources are to be used primarily for business, the company realizes that employees may occasionally use them for personal matters and therefore provides access to non-offensive personal sites during non-business hours:

- Non-business internet activity will be restricted to non-business hours. actively blocks non-business sites during working hours. Working hours are defined as Monday to Friday from 7 a.m.-noon and from 12:45 p.m.-5 p.m.
- The definition of non-business sites is the sole discretion of the IT team. This definition can, and will, change without notice as the internet continues to evolve.
- Internet activity will be monitored for misuse.
- Internet activities that can be attributed to a domain address (such as posting to newsgroups, use of chat facilities and participation in mail lists) must not bring disrepute to or associate with controversial issues (e.g., sexually explicit materials).
- Internet use must not have a negative effect on operations.
- Users will not make unauthorized purchases or business commitments through the internet.
- Internet services will not be used for personal gain.
- Internet users will make full attribution of sources for materials collected from the internet. Plagiarism or violation of copyright is prohibited.
- Release of proprietary information to the internet (e.g., posting information to a newsgroup) is prohibited.
- All internet users will immediately notify the IT team of any suspicious activity.
- All remote access to the internal network through the internet will be encrypted and authenticated in a manner authorized by the IT team.
- Accessing personal social networking accounts (including but not limited to Facebook, Twitter, Google+, LinkedIn, Foursquare and Tumblr) or using email for social networking purposes is prohibited during working

  hours. The use of social networking sites for specific business purposes must be pre-approved or assigned by a manager or supervisor.

Email Security Policy

The Email Security Policy specifies mechanisms for the protection of information sent or retrieved through email. In addition, the policy guides representatives of in the acceptable use of email. For this policy, email is described as any computer-based messaging including notes, memos, letters and data files that may be sent as attachments.

Authorized users are required to adhere to the following policies. Violators of any policy are subject to disciplinary actions, up to and including termination.

The following items are the corporate policy statements for Access Controls:

- All email on the information systems, including personal email, is the property of . As such, all email can and will be periodically monitored for compliance with this policy.
- Individual email accounts are intended to be used only by the person to whom they are assigned. Special arrangements can be made to share information between team members, such as between a producer and an account representative. In all other cases, no user is authorized to open or read the email of another without the express consent of senior management (e.g., chief executive officer, chief operating officer, chief financial officer, CIO or vice president of HR).
- Email is provided to the users of primarily to enhance their ability to conduct business.
- Email will be stored on the system up to a maximum of 750 MB per mailbox. Mailbox is defined as the combined total of deleted items, inbox, sent items and any user-created email folders. Users will receive a warning message stating that they need to clear out space when their mailbox size reaches 500 MB. However, once the mailbox storage space exceeds 750 MB, users will not be able to send new mail messages until the mailbox size falls below the 750 MB limit. In all cases, however, users will continue to receive incoming messages.
- The maximum size of any individual incoming email message will be 20 MB.
- Terminated employees will have all email access immediately blocked.
- Users who leave the company will have all new emails automatically forwarded to their supervisor, or their designated representative, for 30 days.
- The former employee's supervisor is responsible for disseminating stored emails to the appropriate party. Thirty days after the date of termination, the former employee's mailbox will be permanently removed from the system.

The following items are the corporate policy statements for Content:

- Use of profane, inappropriate, pornographic, slanderous or misleading content in email is prohibited.
- Use of email to spam (e.g., global send or mail barrage) is prohibited. This includes the forwarding of chain emails.
- Use of email to communicate sexual or other harassment is prohibited. Users may not include any words or phrases that may be construed as derogatory based on race, color, sex, age, disability, national origin or any other category.
- Use of email to send unprofessional or derogatory messages is prohibited.
- Forging of email content (e.g., identification or addresses) is prohibited.
- All outgoing email will automatically include the following statement: "This email is intended solely for the person or entity to which it is addressed and may contain confidential and/or privileged information. Any review, dissemination, copying, printing or other use of this email by persons or entities other than the addressee is prohibited. If you have received this email in error, please contact the sender immediately, and delete the material from your computer."

The following items are the corporate policy statements for Usage:

- Any email activity that is in violation of policy statements or that constitutes suspicious or threatening internal or external activity will be reported.
- When sending email, users should verify all recipients to whom they are sending the message(s).
- Be aware that deleting an email message does not necessarily mean it has been deleted from the system.

Personal Equipment Policy

This policy provides guidelines for using corporate IT support resources for personally owned equipment and related software, including, but not limited to, notebook computers, desktop computers, personal digital assistants (PDAs), smartphones and

cellphones.

recognizes that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of corporate resources, human or otherwise, for personal gain must be monitored closely.

As a general rule, employees of will not use or request corporate IT resources in the use, network connectivity or installation of their personally owned equipment or software.

Personally owned notebooks and desktop computers will not be granted direct physical access to the network. Employees that wish to access the network from a remote location using their personally owned computer may do so using only -authorized software and only with the approval of their supervisor or manager.

PDAs and smart phones, which include devices using BlackBerry, iPhone, Windows Mobile, Android, Linux and Palm technologies, will be supported according the following rules:

- Employees are responsible for learning, administering, installing and setting up their own PDAs or smartphones.
- Corporate IT resources should not be used for assistance in the basic operation of these devices.
- Upon request, the IT team will install the necessary synchronization software to the employee's desktop or notebook computer.

Virus, Hostile and Malicious Code Security Policy

The intent of this policy is to better protect assets against attack from destructive or malicious programs:

- Any public domain, freeware or shareware software will be evaluated by the IT team prior to installation on any company resource.
- No unauthorized software will be downloaded and installed on end-user machines without express approval from the IT team.
- System users will not execute programs of unknown origin, as they may contain malicious logic.
- Only licensed and approved software will be used on any company computing resource.
- All licensed software will be write protected and stored by the IT team.
- users will scan all files introduced into the environment for virus, hostile and malicious code before use.
- The IT team will ensure that obtains and deploys the latest in virus protection and detection tools.
- All information systems media, including disks, CDs and USB drives, introduced to the environment will be scanned for virus, hostile and malicious code.
- All email will be scanned for virus, hostile and malicious code.
- All internet file transfers will be scanned for virus, hostile and malicious code.
- The unauthorized development, transfer or execution for virus, hostile and malicious code is strictly prohibited.
- All users will report any suspicious occurrences to his/her supervisor or the IT team immediately.
- All company systems will be protected by a standard virus protection system.
- Virus engines and data files will be updated on at least a monthly basis.
- Viruses that are detected on a user's workstation will be reported to the IT team immediately for action and resolution.
- Irregular behaviors of any software program will be reported to the IT team immediately.

BRING YOUR OWN DEVICE (BYOD) AND ACCEPTABLE USE

The BYOD and Acceptable Use Policy applies to all employees, interns, contractors, vendors and anyone using assets. Policies are the organizational mechanism used to manage the confidentiality, integrity and availability issues associated with information assets. Information assets are defined as any information system (hardware or software), data, networks, and components owned or leased by or its designated representatives.

BYOD Policy

This policy provides guidelines for using personally owned devices and related software for corporate use.

The BYOD policy applies to all employees, contractors, vendors, and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or a designated representative.

Furthermore, based on the amount of personally identifiable information employees work with, management reserves the right to determine which employees can use personally owned devices and which cannot.

General Policy

 recognizes that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of these devices must be monitored closely.

The following is a list of personally owned devices permitted by for corporate use:

- Desktop computers
- Laptop computers
- Tablets
- PDAs
- Smartphones
- Portable music players

Reimbursement

 will provide reimbursement for the purchase of personally owned devices up to $_____. However, is not responsible for any additional costs associated with learning, administering or installing these devices.

Registering Devices

All personally owned devices must be registered with the IT department.

End-user Support

As a general rule, users of personally owned devices will not use or request corporate IT resources in the use, network connectivity or installation of their equipment or software. Users are responsible for learning, administering, installing and setting up their personally owned devices.

 IT will support personally owned devices as follows:

- The user will be required to allow IT to load security software on each device.
- The user will be required to allow IT to install remote wiping software on each device.
- Upon request, the IT team will install the necessary synchronization software to the user’s desktop or notebook computer.

Device Security

The user should follow good security practices including the following:

- Password protect all personally owned devices
- Do not leave personally owned devices unattended

Release of Liability and Disclaimer to Users

hereby acknowledges that the use of personally owned devices in connection with business carries specific risks for which you, as the end user, assume full liability.

In the case of litigation, may take and confiscate a user's personally owned device at any time.

Acceptable Use Policy

This policy provides rules for the acceptable use of personally owned devices on the corporate network.

The Acceptable Use Policy applies to all employees, contractors, vendors, and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or a designated representative.

General Policy

Users that wish to access the network using their personally owned computer may do so using only -authorized software and only with the approval of the user's supervisor and the IT department.

Users must follow the same rules when accessing the network from both corporate-issued equipment and personally owned devices. When connected to the network, the user will NOT do the following:

- Use the service as part of violating the law
- Attempt to break the security of any computer network or user
- Attempt to send junk email or spam to anyone
- Attempt to send a massive amount of email to a specific person or system in order to flood a server

Authorization of Devices

IT reserves the right to determine the level of network access for each personally owned device. The user could be granted full, partial or guest access.

IT will install a digital certificate on each personally owned device, which will authenticate the user.

Third-party Applications on Devices

IT reserves the right to block or limit the use of certain third-party applications, such as those that probe the network or share files illegally, that may harm the corporate network.

As the number of approved applications continually evolves, the user must check with the IT department for the current list of approved third-party applications and get IT approval before downloading an application on the device.

Remote Wiping

While does not own the device, it does own all company data. Therefore, reserves the right to remotely wipe the user's personally owned device at any time. Not only will company data get wiped, but the user's personal data could be lost as well. The user must understand and accept this risk.

Furthermore, the user must agree to a full wipe of the personally owned device if he or she leaves . This may result in the loss of both company and personal data on the device.

Reporting Security Concerns

The user agrees to report the following immediately:

- If the device is lost or stolen
- If the device has been attacked with malware, a virus or any other suspicious attack
- Any other security concern with regard to company data

Release of Liability and Disclaimer to Users

hereby acknowledges that the use of a personally owned device on the network carries specific risks for which you, as the end user, assume full liability.

ONLINE SOCIAL NETWORKING

Our company is committed to maintaining a good relationship with employees and with the public. If sustains a positive reputation and excellent image in the public eye, it directly benefits the company as a whole, in addition to putting you in an advantageous situation as an employee. The way the public views is vital to promoting business, gaining new business, retaining first-class employees, recruiting new employees, and marketing our products and services.

While has no intentions of controlling employees' actions outside of work, it is important that employees practice caution and use discretion when posting content on the internet, especially on social networking sites that could affect 's business operations or reputation. This policy serves as a notice on the practice of social networking for all employees to read and understand.

The following is the purpose of the Online Social Networking Policy:

- To guarantee a constructive relationship between the company and its employees
- To reduce the possibility of risk to or its reputation
- To discourage the use of company time for personal networking
- To ensure employees are aware of their actions while engaging in social networking, the number of individuals who can access information presented on social networking sites and the consequences associated with these actions

Definitions

Social Networking

Defined as any activity that involves interaction in online communities of people. This interaction includes, but is not limited to, browsing other users' profiles, browsing other users' photos, reading messages sent through social networking forums and engaging in online communities' instant messaging services.

Social Networking Sites

Specific online communities of users, or any website that links individuals electronically and provides a forum where users can connect and share information. These websites can be general or tailored to specific interests or certain types of users. Examples of popular social networking sites include Facebook, Twitter, Google+, LinkedIn, Foursquare and Tumblr. The list of domains that constitute social networking sites is ever-growing and changing because of the nature of the internet.

Social Networking Profile

A specific user's personalized webpage within a certain social networking site, usually containing personal information such as one's name, birthday, profile photo and interests.

Microblogging

The practice of publishing your recent whereabouts, thoughts or activities on a social networking site for other users to see. This is the main focus of social networking sites such as Twitter, but it also includes features like status updates on Facebook.

Business Purposes

Using a social networking site for the company's gain, usually as a task or assignment given by a manager or supervisor. This can be done either through a specific company account on a given social networking site or through a personal account for the purposes of recruiting or marketing for .

Prohibited Use

It is important that employees use their time while at work to conduct company business. Employees are not blocked from access to social networking sites on computers because, under some circumstances, social networking is a powerful business tool that can be channeled to gain positive publicity for the company and to connect with clients. However, access to such websites does not mean they can be used at any time. The following actions are prohibited during working hours:

- Using social networking sites to conduct personal or non-company business
- Browsing social networking sites for non-company business on company time
- Reading email alerts regarding personal social networking account activity or using email to correspond with personal social networking contacts
- Updating information, uploading photos or otherwise engaging with one's own, personal social networking profile for non-business purposes

- Micro-blogging for a non-business purpose on a social networking site throughout the day, whether it is on a company-provided computer or a personal PDA or smartphone device

Prohibited Conduct

Having your own individual social networking account and using it on your own time is certainly permissible. However, keep in mind that some actions on your personal site are visible for the entire social networking community and are no longer private matters. While will not be continuously monitoring employees' personal conduct on social networking sites, it might be a good guideline to assume that anything posted on your personal social networking profile could potentially be seen by anyone at the company. While this section of the policy is a sensitive one, put it in place to protect not only the company, but you and your job. It is for your own security and defense that you follow these guidelines:

- Do not use microblogging features to talk about company business on your personal account, even on your own time. Do not post anything you would not want your manager or supervisor to see or that would put your job in jeopardy.
- Do not use the company name, address or other information in your personal profile. This is for your physical safety as well the safety of everyone else at the company and the protection of 's name.
- Do not post any pictures or comments involving the company or other employees that could be construed as inappropriate.
- You are also responsible for what other users post on your individual social networking profile. Do not allow inappropriate or sensitive information regarding anywhere on your profile, even if it is generated by a different user.
- Remember that if your personal profile is visible to other employees at the company, supervisors, managers or peers, practice caution. You have control over yourself but not over these employees, and just one inappropriate picture or comment taken out of context could fall into the wrong hands and cost you your job.

Cyber Security Policy: Employee Acknowledgment

Security of information and the tools that create, store and distribute that information are vital to the long-term health of our organization. Likewise, it is imperative that we maintain a positive reputation and excellent public image. To further these objectives, has established this Cyber Security Policy.

All employees are expected to understand and follow the guidelines established by this policy. We encourage employees to take a proactive approach to cyber security. If and when you identify a potential problem, please report it promptly to your direct supervisor.

Prior to using equipment, each employee is expected to have read the entire Cyber Security Policy.

If you have any uncertainty regarding the content of this policy, you are required to consult your supervisor. This should be done prior to signing this acknowledgment form.

By signing below, I acknowledge that I have read ’s Cyber Security Policy in its entirety, and I understand and agree to the requirements and expectations of me as an employee.

Employee signature Date