Contents

Information Security Policies Overview

Running a successful, high-performing organization like THE ORGANIZATION requires reliable, timely information, which is crucial to our continued growth and prosperity. It's also crucial that that information – much of which has been entrusted to THE ORGANIZATION by donors, community members, and others who make our organization possible – be protected at all times. The following policy guidelines outline THE ORGANIZATION's methods for managing and safeguarding this critical data.

Why do we need these policies?

Making sure that information is available when it is needed is essential to THE ORGANIZATION's operation. Rapid and continuing technical advances in information processing have increased THE ORGANIZATION's dependence on information and automated systems, and the value of THE ORGANIZATION's software and data far exceeds the value of its associated hardware. For that reason, information processed by THE ORGANIZATION's computers must be recognized as a major ORGANIZATION asset and be protected accordingly.

Protecting data can mean several things:

1. Physically protecting information-processing facilities and equipment
2. Maintaining computer programs and data integrity
3. Assuring that automated information systems perform their critical functions correctly, in a timely manner and under adequate controls
4. Protecting against unauthorized disclosure of information
5. Assuring the continued availability of reliable and critical information

Who is responsible for implementing and supporting these policies?

THE ORGANIZATION's Security Awareness Policy states that all individuals who access THE ORGANIZATION's computers – employees, contractors, consultants, temporaries and those affiliated with third parties – are responsible for understanding THE ORGANIZATION's Information Security Policies and Standards. We are all accountable for our actions relating to information resources, and are all accountable for the accuracy, integrity and confidentiality of the information we access.

The following sections outline staff roles and responsibilities for protecting ORGANIZATION information according to the established security policies.

Responsibilities of all staff:

1. Protecting THE ORGANIZATION's information
2. Being accountable for the accuracy, integrity, and confidentiality of the information they access

3. Using ORGANIZATION information for authorized company business only
4. Never sharing and/or using information pertaining to ORGANIZATION communications, its customers and/or computer and communication with anyone who is not authorized to use this information
5. Being aware of THE ORGANIZATION's policies related to computer and communication systems security
6. Reporting all security compromises or potential security compromises immediately to their supervisor and the director of information technology

Department managers and the Director of Information Technology have additional responsibilities. See page 18 for additional details.

What are the possible consequences of disregarding these policies?

Any employee of THE ORGANIZATION who willingly and deliberately violates these policies will be subject to disciplinary action up to and including termination.

Others contracted by or for THE ORGANIZATION, such as vendors or suppliers, who willingly and deliberately violate these policies will be subject to business discontinuation and possible legal action.

When and where should these policies be applied?

These policies are applicable when you are:

1. Creating or using THE ORGANIZATION's information
2. Accessing THE ORGANIZATION's computing environment
3. Managing the continuity of your business function
4. Duplicating or modifying THE ORGANIZATION's information
5. Transmitting THE ORGANIZATION's information

These policies and associated standards are applicable across all computing environments and data communication systems owned and/or administrated by THE ORGANIZATION.

What if I need an exception to these standards?

The director of information technology must approve any exceptions to these policies and standards in writing before action may be taken. All renewed exceptions must be approved in writing.

When are these policies reviewed?

Each policy area is reviewed at least annually and standards may be changed or deleted as necessary. Each published policy remains in effect until replaced by a new publication or deleted.

This document supersedes any prior policies and standards at THE ORGANIZATION. These policies and standards are effective immediately for any new systems being developed after MM DD, YYYY.

Existing systems must comply with this policy by MM DD, YYYY.

Computer Usage

All computer equipment and all materials stored on the computer are property of THE ORGANIZATION. There should be no expectation of privacy for information or any materials created, stored or transmitted on ORGANIZATION -owned equipment, including email communications. THE ORGANIZATION reserves the right to monitor computer usage.

THE ORGANIZATION provides security for computer workstations through limited-access authorization and the control of usernames, passwords and group permissions that assure appropriate access to our network and the files stored there. Familiarity with the policies and demonstrated competence in the requirements of the plan are an important part of every employee's responsibilities.

Unauthorized Software and Content

The executive and information technology departments determine what software is loaded on ORGANIZATION computers. No software or freeware should be downloaded by the computer's end user without permission from the information technology department. This includes but is not limited to:

1. File sharing software
2. Internet gaming software
3. Screen savers and background images downloaded from the internet

Adult Content

Transmitting, storing or viewing adult content on any of THE ORGANIZATION's equipment is strictly prohibited. Adult content includes pornography and sex-related merchandise. Child pornography is a federal offense. Anyone with knowledge of child pornography on any ORGANIZATION computer is obligated to report it immediately to the director of information technology.

Maintenance

Users shall never attempt to change or disrupt the configuration or operation of automatic system updates, anti-virus scans, personal firewall settings, or any other process initiated by the Information Technology Department.

Workstation Usage and Security

Usage:

1. All computer users will report potential threats to the computer and to the integrity and confidentiality of data contained in the computer system
2. All computers will be plugged into a surge protector
3. Staff members logging on to the system will ensure that no one observes the entry of their password
4. Staff members will not share passwords, nor login as another user nor enter data under another person's account
5. After three failed attempts to log on, the system will refuse to permit access. Staff must contact tech support to unlock their account
6. Each person using our network is responsible for the content of any data they input or transmit through our system
7. No employee shall access confidential information that they do not have a clear business need to view. No employee shall disclose confidential information unless properly authorized
8. Employees must not leave printers unattended when they are printing confidential information per THE ORGANIZATION's information classification policy

Security:

1. Staff members using the computer network shall not write down their passwords and place them at or near their computers
2. Each computer will have a local policy that generates a screen saver after 10 minutes and requires a password upon resume
3. Users must log off the system when they plan to leave their workstation for more than 60 minutes
4. All computers shall be turned off before leaving the office for the day
5. Users must report any virus activity immediately to the technology department. If you suspect your computer is infected by a virus, turn it off and do not turn it back on until a member of the technology department has inspected it
6. Users shall never store personally identifiable information, credit card information or any other information associated with donors or contributors on their computers

Equipment Checkout

THE ORGANIZATION has some equipment that may be checked out for business use, such as:

1. Portable projector and screen
2. Laptop
3. Presentation mouse

Anyone who chooses to check out equipment must reserve it with information technology at least one week in advance. If administrative staff members wish to check out equipment, their supervisor must authorize the checkout.

Equipment may be checked out for business purposes only, such as when on-site visitors require internet access. Equipment is not available for personal use.

Password Security

Users shall never share their passwords with individuals inside or outside of THE ORGANIZATION, except for with the Information Technology staff when they are troubleshooting an issue with your access or workstation. In addition, users shall never write their password down.

User shall select passwords that:

1. Are at least eight characters long
2. Contain at least one capitalized alpha character
3. Contain at least one lowercase alpha character
4. Contain at least one numeric character
5. Do not repeat a former password

Strong passwords also have the following characteristics:

1. Do not contain your username, real name or THE ORGANIZATION's name
2. Do not contain a complete dictionary word
3. Are significantly different from previous passwords. Passwords that increment (Password1, Password2, Password3) are not strong
4. Contain characters from each of the following four groups: uppercase letters, lowercase letters, numerals, symbols

ORGANIZATION passwords expire every 90 days.

Internet Usage

Users are to practice safe internet browsing behavior that will lower the risk associated with viruses, worms and spyware. THE ORGANIZATION reserves the right to monitor internet usage. Users shall ensure that they manage their business information with the utmost care and never share this information with any outside party unless explicitly authorized by management.

The following guidelines have been established to help ensure responsible and productive Internet usage:

1. Internet data that is composed, transmitted or received via our computer communications systems are considered to be part of the official records of THE ORGANIZATION and, as such, are subject to disclosure both internally and to law enforcement or other authorized third parties. Employees should always ensure that the information contained in email messages and other transmissions is accurate, appropriate, ethical and lawful.
2. Data that is composed, transmitted, accessed or received via the internet must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating or disruptive to any employee or other person. Examples of unacceptable content may include, but are not limited to: sexual comments or images, racial slurs, gender-specific comments, libelous or slanderous information, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation or any other characteristic protected by law.
3. The unauthorized use, installation, copying or distribution of copyrighted, trademarked, or patented material on the internet is expressly prohibited. As a general rule, if an employee did not create material, does not own the rights to it or has not received authorization for its use, it should not be accessed, downloaded, used or distributed in any manner.
4. Abuse of the internet access provided by THE ORGANIZATION in violation of law or THE ORGANIZATION policies may result in disciplinary action. The following behaviors are examples of activities that are prohibited and can result in disciplinary action:
    a. Sending or posting discriminatory, harassing or threatening messages or images
    b. Using the organization’s time and resources for personal reasons or gain
    c. Stealing, using or disclosing any password without authorization
    d. Copying, pirating, hacking, reverse engineering, decompiling, recompiling or downloading software code and electronic files without permission
    e. Sending or posting confidential material, trade secrets or proprietary information outside of the organization
    f. Violating copyright law

g. Failing to observe licensing agreements
h. Engaging in unauthorized transactions that may incur a cost to THE ORGANIZATION or initiate unwanted internet services and transmissions
i. Sending or posting messages or material that could damage THE ORGANIZATION's image or reputation
j. Participating in the viewing or exchange of pornography or obscene materials
k. Sending or posting messages that defame other individuals
l. Attempting to break into the computer system of another organization or person
m. Refusing to cooperate with a security investigation
n. Jeopardizing the security of the organization's electronic communications systems
o. Sending or posting messages that disparage another organization's products or services
p. Engaging in any other unprofessional, inappropriate or illegal activities

Email Usage

Legal Risks

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although email often seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of email:

1. If you send or forward emails with any defamatory, discriminatory, harassing or obscene remarks, you and THE ORGANIZATION can be held liable
2. If you improperly forward confidential information, you and THE ORGANIZATION can be held liable.

By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of email. Legal obligations include:

1. Users shall never open attached email items that appear to be spam
2. Users shall not share personally identifiable information unless authorized explicitly by the donor, a contributor or management
3. Credit card information shall never be shared via email
4. In the event that a donor or contributor shares credit card information via email, the individual who receives the email is required to notify information technology of the event and the email is appropriately contained and disposed of by information technology staff members

5. It is strictly prohibited to send or forward emails containing, defamatory, unlawfully discriminatory, unlawfully harassing or obscene remarks
6. Do not forge or attempt to forge email messages
7. Do not send email messages using another person's email account
8. Do not attempt to disguise your identity when sending email

Email accounts

1. All email accounts maintained on THE ORGANIZATION's email systems are property of THE ORGANIZATION
2. Email is provided for business related communications
3. Email to more than 49 recipients should be sent through means other than Outlook

Mailbox Limits

Mailbox limits protect THE ORGANIZATION's available disk space, backup and restore times, Service Level Agreements and Outlook performance. Mailbox limits help THE ORGANIZATION:

1. Prevent denial of service attacks
2. Manage backup and restore windows
3. Scan for viruses
4. Plan for capacity
5. Mitigate costs
6. Manage system performance

Attachment Limits

Email attachments are limited to 35MB for incoming and outgoing mail. If you need to share a large file with another party use an alternate method, such as Microsoft OneDrive.

Remote Access

It is the responsibility of THE ORGANIZATION's staff, contractors, vendors and agents with remote access privileges to ensure that their remote access connection is given the same consideration as the user's on-site connection to THE ORGANIZATION.

All network activity during a remote session is subject to THE ORGANIZATION's information technology policies and procedures. Remote users will be automatically disconnected from THE

ORGANIZATION's network after 10 minutes of inactivity. The user must then log in again to reconnect to the network.

Data Privacy

Data security measures must be implemented commensurate with the sensitivity of the data and the risk to THE ORGANIZATION if data are compromised. It is the responsibility of the applicable data owner to evaluate and classify data for which he/she is responsible according to the classification system adopted by THE ORGANIZATION and described below. If data of more than one level of sensitivity exists in the same system or endpoint, such data shall be classified at the highest level of sensitivity.

THE ORGANIZATION has adopted the following four classifications of data:

1. **Sensitive data**. Any information protected by federal, state or local laws and regulations or industry standards such as HIPAA, HITECH, FERPA, etc. For purposes of this policy Sensitive Data include but are not limited to:
    a. Personally Identifiable Information (PII) any information about an individual that can be used to distinguish or trace an individual's identity
    b. Protected Health Information (PHI)
2. **Confidential Data**. Any information that is contractually protected as confidential by law or by contract and any other information that is considered by THE ORGANIZATION appropriate for confidential treatment. For purposes of this Policy and the other Information Security Policies, Confidential Data include, but are not limited to:
    a. Non-public personal and financial data about donors, vendors and grantees; such as Social Security Number or Credit Card Data
    b. Human Resources information such as salary and employee benefits
    c. Information received under grants and contracts subject to confidentiality requirements
    d. Law enforcement or court records and confidential investigation records
    e. Information on facilities security systems
    f. Vendor Contracts and invoices
3. **Internal Data**: any information that is proprietary or produced for use by members of THE ORGANIZATION who have a legitimate purpose to access such data.
4. **Public Data**: any information that may or must be made available to the general public with no legal restrictions on its access or use.

Payment Card Industry Compliance

Payment Card Industry Data Security Standard sets the rules for organizations that handle branded credit cards (Visa, MasterCard, etc.) to reduce credit card fraud. This includes protecting cardholder data.

THE ORGANIZATION website provides for secure and Payment Card Industry-compliant credit card activity for donations and gift card purchases. While providing this access we have adopted the following rules to protect cardholder data:

1. All credit card transactions must process through authorized payment solutions via the website
2. No staff member may take credit card information over the phone or in person
3. No staff member may record a credit card number, expiration date, or any card information by writing down such information
4. Staff who observe violation of these rules must report the instance to the Director of Information Technology immediately

Consequences of Payment Card Industry non-compliance

1. Compensation costs. THE ORGANIZATION may be responsible for free credit card monitoring for the compromised customer
2. Legal action
3. Bank fines
4. Federal audits
5. Remediation costs
6. Lost revenue
7. Damaged reputation

Confidential data is typically the data that holds the most value to a company. Often, confidential data is valuable to others as well, and thus can carry greater risk than general company data. For these reasons, it is good practice to dictate security standards that relate specifically to confidential data.

The following details how confidential data, as identified by THE ORGANIZATION, should be handled. This policy covers all confidential data, regardless of location, in electronic or hardcopy of company data, such as printouts, faxes, notes, etc.

1. Storage: Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key, with the key secured.
2. Transmission: Strong encryption must be used when transmitting confidential data, regardless of whether such transmission takes place inside or outside the company's network. Confidential data must not be left on voice mail systems, either inside or outside the company's network, or otherwise recorded.
3. Destruction: Confidential data must be destroyed in a manner that makes recovery of the

information impossible. The following guidelines apply:

a. Paper/documents: cross cut shredding is required. THE ORGANIZATION employs a third-party vendor to destroy our paper that contains confidential and sensitive information. Locked bins are located in the copy room on each floor.
b. Storage media (CD's, DVD's): physical destruction is required.
c. Hard Drives/Systems/Mobile Storage Media: should be turned into information technology for destruction.

4. Use of Confidential Data: A successful confidential data policy is dependent on the users knowing and adhering to the company's standards involving the treatment of confidential data. The following applies to how users must interact with confidential data:
    a. Users must be advised of any confidential data they have been granted access. Such data must be marked or otherwise designated "confidential"
    b. Users must only access confidential data to perform his/her job function
    c. Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information
    d. Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor
    e. Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor
    f. If confidential information is shared with third parties, such as contractors or vendors, a confidential information or nondisclosure agreement must govern the third parties' use of confidential information
    g. If confidential information is shared with a third party, the company must indicate to the third party how the data should be used, secured, and, destroyed
5. Security Controls for Confidential Data: Confidential data requires additional security controls in order to ensure its integrity. The company requires that the following guidelines are followed:
    a. Strong Encryption. Strong encryption must be used for confidential data transmitted internal or external to the company. Confidential data must always be stored in encrypted form, whether such storage occurs on a user machine, server, laptop, or any other device that allows for data storage.
    b. Network Segmentation. The company must use firewalls, access control lists, or other security controls to separate the confidential data from the rest of the corporate network.
    c. Physical Security. Systems that contain confidential data, as well as confidential data in hardcopy form, should be stored in secured areas. Special thought should be given to the security of the keys and access controls that secure this data.
    d. Printing. When printing confidential data, the user should use best efforts to

ensure that the information is not viewed by others. THE ORGANIZATION copiers feature a “secure” printing function that allows users to send print jobs that are securely held on the printer until a code is entered at the machine.

e. Faxing. Do not fax confidential data.
f. Emailing. Confidential data must not be emailed inside or outside the company without the use of strong encryption.
g. Mailing. If confidential information is sent outside the company, the user must use a service that requires a signature for receipt of that information. When sent inside the company, confidential data must be transported in sealed security envelopes marked "confidential."
h. Discussion. When confidential information is discussed it should be done in non-public places, and where the discussion cannot be overheard.
i. Confidential data must be removed from documents unless its inclusion is absolutely necessary.
j. Confidential data must never be stored on non-company-provided machines (i.e., home computers).
k. If confidential data are written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.

6. Enforcement: This policy will be enforced by the executive team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company will report such activities to the applicable authorities.
7. Definitions
   a. Authentication: A security method used to verify the identity of a user and authorize access to a system or network.
   b. Encryption: The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.
   c. Mobile Data Device: A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive or thumb drive.
   d. Two-Factor Authentication: A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens or biometrics, in combination with a password.

Data Backup, Retention and Disposal

This applies to all data classified as sensitive or confidential per THE ORGANIZATION’s information classification policy.

1. Information is not stored longer than it is needed. THE ORGANIZATION’s records retention schedule specifies the retention period for a detailed list of items. This policy is located on the intranet.

2. Information is disposed of securely when no longer needed for legal, regulatory or business reasons.
3. All audit logs (network, database, web, application, server, etc.) are retained for at least one year.
4. Electronic media containing this information must be disposed of in a proper fashion. Depending on if the media is to be reused the media may be destroyed or overwritten. THE ORGANIZATION follows industry best practice guidelines such as National Institute of Standards and Technology for the disposal of media.
5. Paper content containing this information must be disposed of in a proper fashion when it is no longer required for business purposes. All paper media awaiting destruction is stored in secured bins. THE ORGANIZATION employs a third-party vendor to destroy our paper that contains confidential and sensitive information.
6. Media leaving the control of THE ORGANIZATION must be treated differently than media simply being used internally. Any media that leaves the confines of our secure physical location would include staff smart phones, iPads and flash drives. At a minimum, any device connected to our network that leaves our physical location must be password protected. This includes personally owned devices such as smart phones, iPads and flash drives.
7. When technology assets have reached the end of their useful life they should be sent to information technology for proper disposal.
8. The information technology department is responsible for ensuring all media is wiped clean of data before it is donated or disposed.

Social Networking

Social Networking is defined as the use of dedicated websites and applications to interact with other users, or to find people with similar interests to oneself. Examples of such sites include Facebook, Twitter, and LinkedIn. The Communications department of TPF maintains our official accounts on the social networking sites that they have approved.

This policy applies to all staff and board members of TPF.

THE ORGANIZATION respects the legal rights of its employees. In general, what you do on your own time is your affair. However, activities in or outside of work that affect your job performance, the performance of others, or THE ORGANIZATION's business interests or reputation are a proper focus for company policy.

THE ORGANIZATION regards blogs and other forms of online discourse as primarily a form of communication and relationship among individuals. When THE ORGANIZATION wishes to communicate publicly, it has well established means to do so. Only those officially designated by THE ORGANIZATION have the authorization to speak on behalf of the organization.

THE ORGANIZATION maintains a public blog on our website, a Twitter feed and Facebook page. Employees are encouraged to participate by submitting articles or commenting on submissions. To comment, simply access the blog and use the comment feature. Comments are moderated by the Communications team. You can also submit your articles directly to the Communications team for consideration for publication. All topics are welcome.

This policy is intended to give THE ORGANIZATION employees guidelines for using social networks that are not part of THE ORGANIZATION's official blog, Facebook, Twitter or other social media. If you identify yourself on any public forum as an employee of THE ORGANIZATION, be sure to adhere to the following guidelines.

Social Networking Guidelines

1. Employees are personally responsible for the content they publish on blogs, wikis or any other form of user-generated media. Be mindful that what you publish will be public for a long time. Protect your privacy!
2. Identify yourself by name and, when relevant, your role at THE ORGANIZATION when you discuss THE ORGANIZATION or ORGANIZATION -related matters. Write in the first person. You must make it clear that you are speaking for yourself and not on behalf of THE ORGANIZATION.
3. If you publish content to any website outside of THE ORGANIZATION and it has something to do with work you do or with THE ORGANIZATION, use a disclaimer such as this: "The postings on this site are my own and don't necessarily represent THE ORGANIZATION's positions, strategies or opinions."
4. Respect copyright, fair use and financial disclosure laws.
5. Don't provide THE ORGANIZATION's or another's confidential or other proprietary information. Ask permission to publish or report on conversations that are meant to be private or internal to THE ORGANIZATION.
6. Don't cite or reference donors, grantees, partners or suppliers without their approval. When you do make a reference, link back to the source where possible.
7. Respect your audience.
8. Find out who else is blogging or publishing on the topic and cite them.
9. Be aware of your association with THE ORGANIZATION in online social networks. If you identify yourself as an ORGANIZATION employee, ensure your profile and related content is consistent with how you wish to present yourself with colleagues and clients.
10. Be the first to correct your own mistakes. And don't alter previous posts without indicating that you have done so.
11. Try to add value. Provide worthwhile information and perspective. THE ORGANIZATION's brand is best represented by its people and what you publish may reflect on THE ORGANIZATION's brand.
12. You should make sure that your online activities do not interfere with your job.

Responsibilities of Department Managers

1. Making sure that all users are aware of THE ORGANIZATION's policies related to computer and communication systems security
2. Assessing the value and sensitivity of the information and related equipment for risk assessment, information classification and business continuity purposes. Answering such questions as: What information is important to THE ORGANIZATION? Who else would want the information? What are the consequences of losing sole ownership of the information? What are the consequences if the hardware fails?
3. Establishing and maintaining a risk management program, including a risk analysis process that identifies deficiencies and provides for their corrective action
4. Protecting all the information assets stored in and used by their operational area
5. Assuming all associated risks when authorizing the use of company owned information, computers or software
6. Performing or delegating security administration tasks on a regular basis
7. Reporting all suspicious computer and network-security-related activities, security compromises or potential security compromises immediately to the Director of information technology
8. Assigning or determining information asset ownership for all information resources within the department
9. Ensuring participation by all necessary levels of management, administrative and technical staff during planning, development, modification, and implementation of security and risk management policies and procedures
10. Preparing and maintaining a department's Contingency Plan for Information Resources Services Resumption for the continuation of vital information support services in case of disaster
11. Disciplining employees who violate the Information Security Policies and Procedures
12. Making sure that terminated employees access is revoked immediately upon termination
13. Making sure that access is frozen for employees who go on leave and will not be working for a period of time
14. Distributing company security information and providing technical assistance to operating departments as required

Responsibilities of the Director of Information Technology

1. Approving in writing all exceptions to these policies and standards before any action. All exceptions are reviewed quarterly to determine if they are appropriate
2. Monitor all suspicious computer and network-security-related activities, security compromises or potential security compromises
3. Authorizing in writing the sharing and/or use of remote access or other system access information pertaining to ORGANIZATION computers and communications for anyone who is not authorized to use these systems

4. Authorize in writing all computer systems/applications that are exempt from having/using change control procedures
5. Approving the method of extended authentication for network access before its use
6. Authorizing in writing the downloading and/or installation of software obtained from the Internet
7. Conducting investigations into any alleged computer, network security or encryption compromises, incidents or problems
8. Developing/reviewing the security policies, standards, procedures and guidelines that are developed to comply with company policies and generally accepted information systems control requirements
9. Implementing a security program, which includes developing and subsequently monitoring an information system security self-assessment process to be conducted annually
10. Developing information classification guidelines
11. Developing and maintaining a companywide information security awareness and education program
12. Developing and maintaining the overall company minimum guidelines for administration of access control software and procedures
13. Developing and implementing information security review procedures and work programs that support company policies, procedures, standards and guidelines
14. Ensuring information security requirements are incorporated in automated applications through participation in system design meetings and being active in the development of hardware, software and services within company operating departments
15. Conducting investigations and evaluations of emerging information security techniques and services, and coordinating the implementation of appropriate hardware, software technologies and services, and coordinating the implementation of appropriate hardware, software, and services within company operating departments
16. Distributing company security information and providing technical assistance to operating departments as required
17. Participation in each business unit’s risk analysis process
18. Review and evaluate the effectiveness of controls for automated information systems that are either under development of operational, with particular emphasis on major systems