Sample Information Security Policy

Purpose of this Tool

This tool contains sample elements that can be used by small and mid-sized not-for-profits in the creation of an IT Security Policy. As with any policy of this nature, the organization may wish to engage an IT security professional for assistance in developing a policy that is tailored to the organization's size, complexity, risk profile, and objectives

1.) TELEPHONE USAGE AND OTHER BUSINESS SERVICES

Employees should use common sense regarding time spent on the phone for personal reasons. We discourage the use of business services provided at our location for personal reasons. However, if an employee finds it necessary to use business services provided, such as UPS, Federal Express, the fax machine, or other mail services for personal reasons he/she must reimburse the organization for all expenses associated with such use. Obviously, using these services for personal reasons should not interfere with conducting business.

In addition, for the reasons stated in our Conflicts of Interest policy, employees will not use telephones or other business services to conduct other business, political activities, or any other activities which may adversely affect the interests of _____ (name of Organization).

2.) ELECTRONIC COMMUNICATIONS

All employees are required to have a confidentiality disclaimer message at the end of all outgoing emails. It should read as follows:

> CONFIDENTIAL: This electronic message and any attachments may contain confidential information intended only for use of specific recipients. If you believe you have received this in error and are not the intended recipient, we request that you refrain from disseminating, distributing, or copying this communication. If you believe you have received this message in error, please immediately notify us and delete this communication from your system. Thank you.

Employees should consider that e-mail messages could be forwarded, intercepted, printed, and stored by persons other than intended recipients and should use email accordingly. As a supplement to our current email usage policy, we ask that employees not use e-mail to transmit certain types of confidential information to internal employees or outside parties.

Employees may not use email to send or receive confidential information including, but not limited to, credit card numbers, Social Security numbers, and information that could jeopardize_____ and its employees if the information were disclosed to the public.

ELECTRONIC COMMUNICATIONS (continued)

While this is being done to maintain the security of both internal employees and our external clients, we realize that occasionally this sort of information might need to be communicated electronically. If an employee has a business need to transmit or receive confidential information via email, we've implemented a course of action to allow for additional security of this data.

For information that is confidential to the public, but not confidential to our internal staff please follow the guidelines below.

"Sender": Save your file in the appropriate employee's folder, and immediately notify them by email that a confidential document has been placed in their folder. This can be done through any of the office computers, and also through a remote connection.

"Recipient": you will be required to remove the newly saved document from your [network location/link], and save it to a secure location on your individual drive, or within the appropriate folder in the network.

This will increase the security of these documents, and further protect our valuable data. For additional questions, please contact the Manager of Information Services.

We provide electronic communication tools, services, and equipment ("tools") to enable employees to work productively and efficiently. Electronic communication tools include all voice, video and data communication tools including, but not limited to, mail, electronic mail, courier services, facsimiles, telephone systems, voicemail, computers, computer networks, on-line service, web sites or other Internet connections, computer files, video equipment and tapes, tape recorders and recordings, and bulletin boards.

These tools should be used for business-related purposes. Employees should abide by policies and procedures with respect to business and personal use, access and security, and observance of all laws including copyright and trademark laws.

All documents created, stored or accessed by _____ tools, and all communications, including the messages transmitted or stored on or by them, are the sole property of _____. _____ may access and monitor employee documents, communications and files as it considers appropriate.

Online services and the Internet may be accessed only by employees specifically authorized by _____. You should not duplicate or download any software or materials that are copyrighted, patented, trademarked, or otherwise identified as intellectual property unless you have the appropriate rights to that software or materials. When appropriate Internet material is downloaded, it should be scanned using _____'s approved anti-virus software.

Employees are specifically prohibited from:

- Transmitting, forwarding, downloading or knowingly receiving offensive materials and messages.
- Sending or receiving copyrighted materials, trade secrets, proprietary financial information or similar materials without prior authorization.
- Running programs that attempt to identify passwords or codes.
- Using computer or network services to solicit or distribute literature not related to _____ business during working time.
- Placing pictures, attachments, etc. on _____'s computer or network services on occasions when using for personal use.

ELECTRONIC COMMUNICATIONS (continued)

- Using computer or network services for commercial purposes.
- Sending mass (i.e., more than five recipients) email or messages locally or over the network such as chain letters, advertisements or solicitations. (If you receive a chain mail message, you must reply to the sender asking him/her not to send chain email. You should delete the message without forwarding it.)
- Knowingly installing or running a program that will damage or place an undue burden on the system.
- Knowingly acting in a manner that will disrupt normal operations of the system.
- Using the systems to make statements on behalf of _____, its positions on any issue, unless previously approved in writing by _____.
- Downloading software from the internet without permission from _____.

The above list is not all inclusive. In general, all relevant policies, including Conflicts of Interest, Policy against Harassment, Confidentiality and the like apply to your use of electronic communications tools.

All electronic communications tools are to be used primarily for business purposes. You must use these in accordance with their access privileges. Occasional personal use of these tools is allowed only if it:

- is incidental in nature;
- does not interfere with _____'s business/is not detrimental to;
- does not affect productivity, quality or customer service;
- does not create a conflict of interest;
- does not contribute to personal financial gain;
- is not in violation of any local, state or federal laws;
- is otherwise in compliance with _____'s policies.

You are responsible for:

- Protection of your password.
- Reporting any breach of system security.
- Reporting unauthorized use of your account.
- Changing password on a regular basis.
- Managing mail files by deleting/discarding appropriate messages.
- Detaching attachments on emails to save file space.

You should ensure that no personal electronic correspondence sent could be construed as an official communication of _____ since you may be perceived as representative of _____ and, therefore, damage or create liability for _____.

If you use _____'s tools, the use creates no expectation of privacy. _____ reserves the right to monitor any and all electronic communications, to access all records within it, and to retain and dispose of these records as it deems necessary. Even if you use a personal password or code to access these systems, all messages, documents, or any other material created, or composed, sent or received are not your private property; they belong to _____.

ELECTRONIC COMMUNICATIONS (continued)

Improper use of electronic communications tools will result in discipline, up to and including termination. Improper use includes any misuse as described in this policy as well as any harassing, offensive, demeaning, insulting, defaming, intimidating, or sexually suggestive written, recorded, or electronically transmitted messages. The determination of misuse or improper use is solely at the discretion of _____. If there is a question of whether use is proper or improper, you should consult with your supervisor for clarification.

3.) ACCESS PRIVILEGES TO NETWORK

Any computer used to access our network must have an active anti-virus program. This includes personal/home computers that might have access to our remote servers. If you would like to access our network via a remote connection, please contact the Manager of Information Services to allow for anti-virus software verification prior to establishing a connection to our network.

Users with remote access to servers, and with company issued laptops and mobile devices, should not store passwords to log into their sessions. Storing the passwords can provide unauthorized individuals direct access to your computer, and our network.

Social Media

As of 3/25/20XX _____ distributed a Social Media Guide to all employees. [Link]

Review of IT Access Privileges

Access privileges are reviewed at the arrival and departure of any _____ employee. Appropriate access is given to new employees based on the "New Hire Checklist," which is dependent upon their role in the organization.

When an employee departs, all access privileges are removed according to the "Exiting Employee Checklist," immediately following their last day of employment with _____.

If an employee needs access to a _____ IT resource that they do not currently have, they can contact their supervisor and or the person who oversees the resource, who can formally request access by contacting the _____ Manager of IT. If you have been given access to a resource that you no longer need, notify your supervisor, and the IT manager, immediately so proper access privileges can be restored.

In addition to reviewing access privileges when employees arrive and depart, _____ will also perform a biannual review. Access privileges to _____ network resources will be reviewed and adjusted accordingly, and documented here: (link).

4.) BACKUP AND RESTORATION PROCEDURES

The retention of _____ data in the Backup is:

1. Base image
2. Intra-day incrementals (for last 2 days at every 15 minutes)
3. Daily synthetics (for last 14 days)
4. Weekly synthetics (for last 5 weeks)
5. Monthly synthetics (all)

After the base image is created, the incrementals take place at the frequency above. If we selected 24/7 backups at 15-minute incrementals, that will create 96 incremental files each day. All of these incrementals will be saved on the Backup but only one image is pushed off-site daily to the co-location facility.

Synthetic Incrementals

Incremental files are collapsed into synthetic incrementals (basically a larger incremental file). This is done to ensure chain integrity and to speed up restorations. The fewer hops from the current point-in time back to the base image, the faster your restoration will be.

Recovery after a Catastrophe

A detailed Back-up and recovery document created in conjunction with SecureNA (_____'s IT support vendor) can be found here: _____ (link).

If a disaster results in us losing the entire _____ office — servers and on-site BDR included — we follow a disaster process (link) to order a newly imaged BDR with the most current backup to be shipped out via next business-day air transportation to a location we determine (likely _____ secondary location).

Disaster Recovery and Costs

When the Backup arrives, with the 10Mb Internet access connection in our secondary location, we can simply plug in the patch cable to bring our _____ network up. We are allowed to use the Backup for two weeks before it must be returned to SecureNA. This timeframe should allow us to get a new server ordered, in place and perform a bare metal restore from the Backup before returning it. Alternatively, we can choose to keep the Backup, and we will be billed for the list price of the new Backup.

Standby Server Using Instant Virtualization

The Backup has the ability to create a standby of a failed server by creating a virtual image of the failed server on the Backup. This unique ability is due to the fact that the virtualization engine natively understands the backup images as a hard drive allowing a failed server to be virtualized within minutes. The "virtualized" server retains the same IP address, NetBIOS name, MAC address and application state of the original server. Once virtualized, the standby server will resume the backup schedule that was in effect before the failure.

Bare-Metal Restore (Virtual to Physical)

When it comes time to restore the virtualized server back to physical hardware, we will use a bare-metal restore process, which allows restorations to dissimilar hardware. We use a boot disk that can be used with the new server to trigger the restore process. This allows us to restore the server image onto the new server while adding the new drivers necessary for that server.

Monitoring and Management

Our _____ Backup is monitored and managed 24/7 by _____ service provider. If a problem occurs during any backup or with the hardware, they are alerted and take corrective action.

Website Back-up/Recovery and Uptime

Our website is hosted by X. Their backup configuration is as follows:

- X has a dedicated server with Rackspace, one of the largest hosts in the world
- A third-party vendor monitors the server 24/7, letting X know if there are any issues or downtime
- A third-party vendor provides 24/7 server maintenance to help resolve any server-related issues and to make sure they're performing at peak performance
- Servers RAID, meaning there are multiple disk drives providing redundancy in the case that one drive goes down
- Daily off-site backup where the server is cloned and moved to an off-site location in case something happens to the physical facility of the primary server
- Over the past year, the server has had over 99.9% uptime
- X provides phone and email support on the Content Management System in the event the client has questions regarding how to update or expand content on the site.

Our agreed upon expectations of customer service with X are outlined here: (link) _____ Customer Service Memo 20XX