

Sample Office Digital Security Policy

Modify the contents of this document as needed to meet local ordinances and established laws in your area. This document is not meant to replace other legal and binding pre-existing documentation. It is meant to be a starting point only. Print it out and have it signed by all employees that may come into contact with any information assets in your department. Store in a secure location and review with your employees annually. Reviewing and renewing annually will allow you to modify the contents to reflect your ever changing security issues.

What Is A Security Policy

The security policy is basically a plan, outlining what the office's critical assets are, and how they must (and can) be protected. Its main purpose is to provide staff with a brief overview of the "acceptable use" of any of the Information Assets, as well as to explain what is deemed as allowable and what is not, thus engaging them in securing the office's critical systems.

The document acts as a "must read" source of information for everyone using any systems and resources defined as potential targets. A good and well developed security policy should address some of these following elements:

- How sensitive information must be handled
- How to properly maintain your ID(s) and password(s), as well as any other accounting data
- How to respond to a potential security incident, intrusion attempt, etc.
- How to use workstations and Internet connectivity in a secure manner
- How to properly use the e-mail

Basically, the main reasons behind the creation of a security policy is to set a office's information security foundations, to explain to staff how they are responsible for the protection of the information resources, and highlight the importance of having secured communications while doing business online.

The perfect Digital Security environment is an unattainable myth. What's important is to stay focused on and improve our security practices to reduce the possibility of data compromise.

What follows is an example Office Digital Security Policy.

Office Digital Security Policy

The use of office digital equipment, or personally owned digital equipment on the office network, falls under the guidelines below:

Transference

Transferring private data from within the organization to another location outside the organization is prohibited except in the performance of your duties. Any information transmitted that is defined as organizationally private should be encrypted and sent via secure email or postal carrier. Other information relating to the inner workings of office digital security (passwords, encryption keys, procedures, etc) should be kept confidential. Information posted to internet connected servers should only be transferred if the website uses encrypted communications. If in doubt, contact your supervisor.

Media

Media is defined as CD-R or RW, DVD-R or RW, USB Flash Drives, Floppy disks, Backup Tapes or any other means of storing data. Personal media should not be used for which to copy any organizational data. Any requests for removable media will be monitored so as to insure employees are not removing the media from the premises. Offsite backups should be stored in a secure lockable location. Your local bank can supply a quality secure storage location for a nominal fee.

Server Backups

Server backups will only be run by qualified backup operators. Any media that is used in a server backup (examples above) should be taken off site at least once a week along with any backup logs that detail them. Access to these backups will be restricted to backup operators or supervisors.

Personal Backups

If you backup documentation from your workstation the media will not be allowed offsite except for the purposes of offsite disaster recovery (see media above).

Proxies

Web proxies that obscure your browsing activities is strictly prohibited. Some of these proxies can monitor any and all traffic passing through them capturing confidential organizational data.

IM and CHAT

Instant messaging and chat clients are usually not very secure. The data transferred is normally not encrypted and can be intercepted in route. Chatting about office business on an IM or Chat client is strictly prohibited. Instant messaging family or friends during work hours is also discouraged. These messaging clients can have security vulnerabilities and they can be compromised by tech savvy hackers. This can give them access to the internal network and compromise office security.

EMAIL

Office email is a valuable resource. It is also probably the weakest link in any organizations security. If you need assistance, contact your supervisor.

- Do not use your work email address to register for any personal web related processes.
- Do not use your office email account to stay in contact with family or friends.
- Passing jokes or funnies between email accounts can subject your computers and network to data compromise.
- Purging your deleted emails and exporting sensitive emails to a folder on your desktop is recommended.

- Turning off the preview pane in your email client is also recommended.
- Using unencrypted web based email clients for official business is prohibited.

Web based email accounts like Hotmail, Google, etc have the ability or is already encrypted. If you must use web based email then you should confirm that you are connecting via secure connection.

Online Games

Participation in online gaming is discouraged. Game sites are potential sources of virus attacks and intrusion attempts. When you are connected to play checkers with someone else on the internet there are open connections into your computer that can be compromised.

Usernames and Passwords

All workstation access must be password protected. If you do not have to use a password to get into your computer, please inform your supervisor. Supervisors must be made aware of your workstation password to facilitate normal operations in your absence. Supervisors should keep a pencil and paper log of all usernames and passwords in a secure location.

Station Security

If you must leave your station, you should lock your session by pressing Ctrl-Alt-Del then Enter. Setting your screensaver to password protect on resume is highly recommended.

Installing Software

Download and installing software, screen savers, etc, from internet sources is prohibited. Exceptions to this include operating system updates like Windows Update and updates/software related to the performance of your duties.

Antivirus and Antispyware Software

Attempts to circumvent or remove any antivirus or antispyware protective software is considered a serious violation. The computer user has the responsibility to report any errors with said software and is tasked with insuring it remains updated. If you have questions about how to confirm this please ask your supervisor.

Compromise

If you suspect you have a virus, spyware, or you think you may have a security issue of any nature, you must report it to your supervisor immediately.

Use during Breaks, Lunch, and After Hours

This policy extends to all use of office digital equipment during all hours of the day and night. This policy also applies to any personal computing devices, laptops, PDA's, etc that may be connected to the Office network.

Employee

Date