Facilities, Technology, and Equipment Policy and Procedure Manual

Operation Threshold
7/21/2011

Violation of these Operation Threshold polices and/or procedures will result in disciplinary action up to and including termination.

Keycard Access

- Please safeguard your assigned keycard that gains you entrance into the central office building.
- Do not loan your key card to others as each individual card granted specific authorities.
- All times are logged into the system.
- If you have problems with your keycard please contact the IT Manager.
- If you lose your keycard, you must contact someone from the IT Staff immediately, replacement fees will apply.
- The IT Manager's office phone rolls over to a mobile phone after hours: (319) 292-1874. You should make all reasonable efforts to speak with the IT Manager, and should leave a message only if you are unable to reach someone. In the event that you are forced to leave a message please contact your Department Director or the Executive Director (319) 239-4049) as well.

Shoretel Phone System

- For all Shoretel phone issues please contact the IT Manager.

General Computer Access

Your workstation and the contents are the property of Operation Threshold and are provided to you for agency purposes. Do not engage in activities that could permit your workstation and the Operation Threshold network to be compromised by computer viruses, malware or hackers.

The combination of username and password define the identity of all users on the system. This information is known as your network account and has been created to protect your privacy and the integrity of your electronic files.

Password Requirements

All passwords must use a combination of alpha, numeric and/or special characters, and be a minimum of five (5) characters in length (e.g., time2go, cat$fish, only1ofme). The network will automatically prompt you to change your network password. You may choose to change the password more often if you desire.

Logging Out

Log-out or lock your workstation if you leave your computer unattended. Many computers can be locked by pressing CTR-ALT-DEL simultaneously and selecting the 'lock workstation' option. When you return to your computer, simply re-enter your password to resume use.
Screensavers can be used to automatically protect your PC and network account from unauthorized use. Generally, you can unlock your screensaver using the same password that you used to log-in.

Resetting Passwords

You can re-establish a password you have forgotten or had been disabled by contacting the IT Manager.

Computer Operation

Power-off your computer and monitor when you leave work for the day or weekend, and at any time your computer will not be in use for long periods of time.

- Always power-off your computer by using the operating system menus. Never use the power button to shut down your computer. Doing so may corrupt open files and the operating system.

- You may shut down monitors, printers and other 'non-intelligent' devices by using the power switch. Always power-off your computer before turning off any other connected devices.

- Please leave your computer on, but logged off, on Wednesdays. This is when the updates will occur.

Virus Protection

Operation

Every computer is protected by an anti-virus protection program. You are strictly prohibited from disabling, removing or modifying the program or its settings. Doing so could cause irreparable harm to the system and data.

Virus alert/Infection

If your screen displays a message stating that your computer is infected with a virus, call the IT Staff immediately.

Wireless & Guest Access

Wireless connectivity provides significant flexibility and mobility when you need to use laptop computers, PDAs, keyboards and other devices. However, wireless connectivity introduces a significant security risk to computer networks and data.

- Operation Threshold manages all wireless devices to protect network services from interruption or data loss.
- Wireless services must have all reasonable security features such as encryption (security) and authentication (identification) enabled.
- Employees are not authorized to install any wireless access points on our system.
- We recommend you use a network cable if you are close to a wall jack; this is the preferred method to connect to the network, it is much faster and more secure. If you need wireless access on a new device please see the IT Staff.
- Non Operation Threshold computers are not allowed to plug into a physical Ethernet port. Non Operation Threshold workstations, or any device not secured by the IT department, may connect to the OTtemp wireless network; however, the workstation needs to have an updated antivirus software package with the latest definitions installed before connecting to our network. The OTtemp key changes regularly, please see the IT Manager for the latest key.

Files and Applications (Downloading)

Files available for downloading over the Internet or via CDs, floppy disks, memory keys and other portable media can be divided into two general groups. The first group can be defined as *data files* and may contain documents, files or other stored information. The other group can be defined as *application programs* and may contain new software products, tools or applications that can be loaded onto a computer.

Data Files

You may transfer work related data files only to and from Operation Threshold computers. If you use a USB Stick to move data between Operation Threshold workstations, please be sure to erase that information from the USB Stick after you have copied it.

You may not store sensitive or restricted Operation Threshold data on your home computers or laptops.

- Restricted or sensitive data about employees, clients, or anyone otherwise affiliated with Operation Threshold can only be stored on Operation Threshold equipment. Personal or sensitive data includes, but are not limited to, Social Security Numbers, credit card information, name, address, and other personal identification information.

- All Operation Threshold laptops will be encrypted. If your laptop has not been encrypted please contact the IT department so they can set that up. If your computer is encrypted it will ask for a password before it even opens up Microsoft Windows.

Application Programs

You may not download or install any application software to any computer, PDA, system or device that is considered part of the Operation Threshold computer network without explicit direction by IT Staff. This is necessary to protect the integrity of system operations and to meet all legal requirements.

- You may not copy or duplicate software, or the media containing software, to another computer. Doing so is a licensing violation.

- You may not download public domain software (freeware, shareware, etc.) unless approved or provided by IT Staff. Public domain software may contain undesirable code (spyware, adware, etc.) that can interfere with the operation of your computer. In addition, the use of public domain software may be regulated and downloading could violate licensing or distribution agreements.

- You may not install any non-company related software on your computer unless approved by your Department Director and the IT Manager; this includes Skype or any similar software, Music/Video Services, News Services, Weather Applications, File Servers, Toolbars, etc.

- Your computer will be routinely scanned and reviewed for security vulnerabilities and software compliance.

- Installation of Applications:

    i. For all applications that require a license, Operation Threshold must own the license. No personally owned software can be installed on your workstation without the approval of your Department Director and the IT Manager.

ii. The IT department will install all common applications required for business purposes.

- Please contact the IT Manager regarding applications and upgrades.

Hardware or Software

Purchasing

We maintain a set of standard hardware and software products that have proven compatibility and cost value. Purchasing these products is generally faster and requires less work. Having our systems standardized makes it possible for the IT staff to respond to issues in a timely manner. Please have your Department Director contact the IT Manager if you need to make any hardware or software purchases.

Personally-Owned Hardware and Software

You may not install, connect or use personally-owned hardware or software with Operation Threshold systems at any time. The use of personally-owned products can compromise the security and integrity of Operation Threshold data. In addition, such action could violate copyright or license agreements.

Security

Employee Responsibilities

As an Operation Threshold employee, you are responsible for ensuring the security and integrity of the data on all computer systems you use. You are expected to make all reasonable efforts to safeguard all electronic systems by securing terminals and networks from easy access by the public. This may require securing building doors or relocating equipment that could be easily stolen or accessed.

Theft or Loss

You should immediately call the IT Staff to report any lost or stolen equipment. You should make all reasonable efforts to speak with the IT Manager, and should leave a message only if you are unable to reach someone. In the event that you are forced to leave a message please contact your Department Director or the Executive Director (319) 239-4049) as well.

Internet Access and Electronic Communications

Operation Threshold provides its users with Internet access and electronic communications services as required for the performance and fulfillment of job responsibilities. These services are for the purpose of increasing productivity and client service.

Occasional and reasonable personal use of Operation Thresholds Internet and e-mail services is permitted, provided that this does not interfere with work performance. These services may be used outside of scheduled hours of work and during breaks, provided that such use is consistent with professional conduct and with supervisory permission. If you need access to a website that is blocked or any network permissions changed then your request may be granted provided you email your request to your Department Director. If they approve then they will email that change request to the IT staff. Generally request should not be made for personal use; although exceptions may be granted under specific situations.

Violations of Internet/Network and E-Mail use include, but are not limited to.

- Streaming Media (videos, music, TV, News, Movies) that is not business related during regular work hours. Doing this uses up precious internet bandwidth that is planned for business related use.

- Downloading and/or installing software on your computer without your Department Director and the IT Managers approval.

- Accessing, downloading, uploading, saving, receiving, or sending material that includes sexually explicit content or other material using vulgar, sexist, racist, threatening, violent, harassing, discriminatory, or defamatory content.

- Users should not use Operation Threshold's services to disclose corporate or client information without prior authorization or send/post information that is defamatory to the company, its products/services, colleagues and/or clients.

- Gambling and/or any illegal activities.

- Downloading, copying or pirating software and electronic files (e.g., mp3 .avi .mp4 etc.).

- Hacking into unauthorized websites or into the company's own servers and equipment.

- Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems.

- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.

- Installing Toolbars, wallpapers or other programs that could slow down or infect your computer.

We have not included every possible violation, but please be diligent with your use of company resources.

Abuse of the e-mail or Internet systems, through excessive personal use, or use in violation of the law or Operation Threshold polices and/or procedures will result in disciplinary action. Operation Threshold does not intend to regularly review employees' e-mail, Internet and electronic records, however it can and employees have no right or expectation of privacy in electronic information. (Whether done on work time or regular scheduled time.)

If an employee is unsure about what constitutes acceptable Internet / Network and email usage, then he/she should ask his/her Department Director for further guidance and clarification.

Social Media

Social Media is a type of online media that expedites conversation and allows users to participate in the creation or development of content.

Social Media in the Workplace

Operation Threshold embraces the concept of social media as a business tool for purposes of recruiting staff, volunteers, participants, publicizing agency activities and promoting the agency. For those purposes, only a few positions within the agency are allowed to access social media sites on work computers and only for work purposes.

Social Media "Outside" the Workplace

Activities in or outside of work that affect your job performance, the performance of others, or Operation Threshold's reputation and business interests are a proper focus for company policy. Employees need to understand that what is posted on line is permanent and most likely is public. Employees need to remember that they are bound by all agency policies that include but are not limited to anti-harassment, confidentiality, and conduct standards. Careless use of social media can easily result in policy violations, even if the employee does so during non-work time and using personal equipment. Even while engaging in electronic networking outside of workplace, employees must use care not to engage in communications that are of a defamatory, harassing or libelous nature, either against colleagues, supervisors, program participants, vendors, the agency or its programs.

Care must be taken to avoid breaking confidentiality of employees or participants in our programs. Employees should not use social media in any way that crosses professional boundaries with families they serve.

SmartPhones

Personal Smartphones are not managed by Operation Threshold. You may use your smartphone to connect to the Operation Threshold email system for your convenience, provided that you:

Have approval from your Department Director and Executive Director.

All Operation Threshold staff who own a smartphone that synchronizes information with OT resources, are responsible for securing their device to prevent sensitive data from being lost or compromised, viruses being spread, and other forms of abuse. If a Smartphone is lost, stolen, or believed to be compromised, the incident must be reported to the IT manager immediately.

Please contact the IT Staff for connectivity instructions. They will also need to verify you have the security setup on your mobile device.

The Operation Threshold IT staff may be able to help if you have some questions, however if we are not familiar with your model then you may need to contact your cell phone provider.

Protect Your Mobile Device

To ensure that data accessed through your mobile device is secure, especially in the event that it is misplaced, stolen or believed to be compromised, all smartphones synchronizing with OT resources are subject to the following:

- A "PIN" or “Password” consisting of at least 4 characters.
- The timeout for the PIN should be set to a minimum of 30 minutes. Some devices allow this setting to be adjusted to be more or less than 30 minutes.
- A user is allowed 10 attempts to enter the PIN correctly. If the PIN is entered incorrectly 10 times, the device will be reset to "factory settings" or wiped. This is available on some Smartphones.
- Password should be changed periodically.
- Encryption should be enabled on the device If your device supports encryption, enable it and make sure that your sensitive documents are encrypted. Some devices will automatically encrypt these documents and others will present you with the option.

Install Antivirus Software

Although rare, mobile devices are just as susceptible to viruses as desktop or laptop computers. Industry analysts expect viruses, Trojans, spam, and all manner of scams to increase dramatically

as the demand and use of mobile devices grow. Not all mobile devices have antivirus software, but a number of vendors do offer antivirus and anti-spam solutions for some devices.

Please contact the IT Staff for connectivity instructions. They will also need to verify you have the security setup on your mobile device.

The Operation Threshold IT staff may be able to help if you have some questions, however if we are not familiar with your model then you may need to contact your cell phone provider.