

POLICY

This policy provides management and users with guidelines that will protect and improve computer systems, network infrastructure, and information within Mid. The enclosed policies and directives have been established in order to protect the information systems investments and safeguard the information contained within these systems.

PRIVACY DISCLOSURE

Mid cannot and does not guarantee user privacy. Users should be aware that on occasion authorized personnel have authority to access individual user files or data in the process of performing repair or maintenance of equipment. Additional safeguards are in place to monitor Internet downloads and website usage.

PROCEDURE

Contents

1. Statement of Responsibility
2. Access Codes and Passwords
3. The Internet and E-mail
4. Computer Viruses
5. Physical Security
6. Copyrights and License Agreements

1.Statement of Responsibility

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

Department Leader Responsibilities

Managers and Supervisors must:

1. Ensure that all appropriate personnel are aware of and comply with this policy.
2. Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

Network Administrator Responsibilities

The Network Administrator(s) must:

1. Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
2. Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.

Employee responsibilities

Employees are responsible to:

1. Read the policy and have an understanding of all employee responsibility sections of this policy.
2. Comply with all applicable policy

Violations

Violations may result in disciplinary action in accordance with Human Resources Disciplinary Process.

2.Access Codes and Passwords

The confidentiality and integrity of data stored on company systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

Network Administrator(s) responsibilities

The Network Administrator(s) shall be responsible for the administration of access controls to all company computer systems. The Network Administrator(s) will process adds, deletions, and changes upon receipt of a request from the end user.

The Network Administrator(s) will maintain a list of administrative access codes and passwords and keep this list in a secure area.

Employee responsibilities

Each employee:

1. Shall be responsible for all computer transactions that are made with his/her User ID and password.
2. Shall not disclose passwords to others within or outside the company. Passwords must be changed immediately if it is suspected that others may know them. Passwords should not be recorded where they may be easily obtained.
3. Should use passwords that will not be easily guessed by others.
4. Should log out when leaving a workstation for an extended period.

Department Leaders responsibility

Managers and supervisors must notify the Human Resource Leader promptly whenever an employee leaves the company or transfers to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

Human resources responsibility

The Human Resource Leader will notify the Network Administrator(s) of employee transfers and terminations. Involuntary terminations must be immediately reported concurrent with the termination.

3. Internet and E-mail

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide.

Policy

Access to the Internet is provided to employees for the benefit of *Mid*. Employees are able to connect to a variety of business information resources around the world.

Conversely, the Internet also contains many risks and inappropriate materials. To ensure that all employees are responsible and productive Internet users and to protect the company's interests, the following guidelines have been established for using the Internet and e-mail.

Acceptable use

Employees using the Internet are representing the company. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using Web browsers to obtain business information from commercial Web sites
- Internet research and data collection
- Accessing databases for information as needed
- Using e-mail for business contacts
- Agency approved social marketing websites (Examples: Agency Facebook, United Way Facebook)

During your work day, the following is unacceptable use. This applies to all work computers, company mobile devices, and personal mobile devices.

Employees must not use the Internet for purposes that are illegal, unethical, harmful to the company, or nonproductive. Examples of unacceptable use are:

- Sending or forwarding chain e-mail, i.e. messages containing instructions to forward the message to others.
- Conducting personal business using company resources.
- Transmitting any content that is offensive, harassing, or fraudulent.
- Receiving any content that is offensive, vulgar or inconsistent with the values and mission of *Mid*.
- Downloading programs from the Internet
 - This includes but is not limited to:
 - Pornography sites
 - Gambling sites
 - MP3 files/Sound files/Music downloads
 - Any and all peer-to-peer (P2P) file-sharing sites, applications or services
 - Webshots, Hotbar, or any kind of Screensaver programs
 - Downloading anything from screen pop-up ads
 - Chat room services of any type, unless otherwise approved by your direct supervisor
 - Do not use the Internet to listen to **on-line radio stations**. This takes up unnecessary bandwidth and slows down the DSL connection for other users
 - Accessing personal social networking websites such as Facebook and My Space – If you have a Facebook or MySpace page -- You are responsible for all content posted – Confidential agency business or staffing matters should never be shared on a public information source
 - Accessing websites to make personal income (pogo, eBay)
 - Downloading on-line games to your PC/laptop
 - On-line video streaming should only be used for work-related matters such as legislative updates and web conferencing
 - Just a reminder that no programs should be downloaded off the Internet without approval by your network administrator or your supervisor. If you want to download any program off the Internet please get prior approval
- Using a **public** instant messaging service (MSN, Yahoo) unless for business use. This must be approved by your supervisor and Network Administrator.

Protocols for users and their Microsoft Outlook mnca.net accounts

Your mnca.net account is for work-related use. Do not forward **non-work related** e-mail to anyone with a mnca.net account. This activity clutters up our Exchange Server, makes things run more slowly, and can result in system failures or crashes.

On a monthly basis, users will clean up their inbox and empty their deleted and sent items folders. Any unwanted e-mails that are coming into your inbox should be added to the Junk-Email bin.

When sending agency e-mail, please use a standard white background for e-mail templates. Downloaded stationary templates are prohibited.

Downloads

Any file downloads from the Internet are NOT permitted unless specifically authorized in writing by your Network Administrator

Employee responsibilities

An employee who uses the Internet or Internet e-mail shall:

1. Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.
2. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employee's name attached.
3. Not transmit copyrighted materials without permission.
4. Know and abide by all applicable *Mid* policies dealing with security and confidentiality of company records.
5. Avoid transmission of nonpublic customer information. If it is necessary to transmit nonpublic information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.

Copyrights

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express written permission to do. Failure to observe copyright or license agreements may result in disciplinary action by Mid and/or legal action by the copyright owner.

Monitoring

All messages created, sent, or retrieved over the local company network and out to the Internet are the property of the company and may be regarded as public information. *Mid* reserves the right to access the contents of any messages sent over its facilities if the company believes, in its sole judgment, that it has a business need to do so.

Mid reserves the right to monitor all company network traffic. All inbound and outbound Internet traffic may be monitored and/or logged at any time by a network firewall appliance, proxy server, or other technology (OpenDNS).

Approved network administrators are the only staff permitted to access and view recorded communication, and must get approval from the Chief Executive Officer/Executive Director in the event of an ongoing investigation.

All communications, including text and images, can be disclosed to law enforcement and other third parties without prior consent of the sender or the receiver. **This means don't put anything into your e-mail messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.**

Retention Policy

Mid will retain all company electronic communications for as long as deemed necessary for security and policy purposes.

4. Computer Viruses

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources. **The term *virus* in this Manual refers to any form of malware: viruses, worms, Trojans, rootkits, adware/spyware.**

Background

It is important to know that:

- Computer viruses are much easier to prevent than to cure.
- Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

Network Administrator(s) responsibilities

Network Administrator(s) shall:

1. Install and maintain appropriate antivirus software on all computers.
2. Respond to all virus attacks, destroy any virus detected, and document each incident.

Employee responsibilities

These directives apply to all employees:

1. Employees shall not knowingly introduce a computer virus into company computers.
2. Any associate who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and notify the network administrator.

5. Physical Security

It is company policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

Employee responsibilities

The directives below apply to all employees:

1. Diskettes or other storage media (e.g., USB memory stick) that contain highly sensitive or confidential data must be locked up and/or encrypted (e.g., EFS, BitLocker, TrueCrypt, encrypted-Zip file).
2. Diskettes should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
3. Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS). A UPS and/or surge protector shall protect other computer equipment.
4. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
5. Since the Network Administrators are responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by the Network Administrator.
6. Employees shall not take shared portable equipment such as laptop computers out of the office without the informed consent of their supervisor. Informed consent means that the supervisor knows in advance what equipment is leaving, what data is on it, and for what purpose it will be used.
7. Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result. Damage or loss due to negligence will be considered a serious offense.
8. All mobile devices (PDA's, etc.) that contain highly sensitive or confidential data need to be password protected before leaving the facility.
9. Network devices, including but not limited to wireless (WiFi) access points, hubs, switches, routers, must be approved, configured, and installed by Network Administrator. Wireless (WiFi) access points must meet the following criteria for approval:
 - a. Must have encrypted communications using WPA (TKIP), WPA/WPA2 (TKIP/AES) or WPA2-Only (AES). The passkey must be at least 15 characters. WPA2-Only is strongly recommended unless compatibility with older clients is required.
 - b. Open wireless (no security) or WEP security are strictly forbidden.
 - c. On a larger or more advanced network (e.g., Windows Active Directory domain), access point must be isolated on a guest VLAN separate from main LAN.

6. Copyright and License Agreements

Legal reference

Mid and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U.S. code) and all proprietary software license agreements. Non-compliance can expose *Mid* and the responsible employee(s) to civil and/or criminal penalties.

Scope

1. This directive applies to all software that is owned by *Mid*, licensed to *Mid*, or developed using *Mid* resources by employees or vendors.

2. Furthermore, confidential or proprietary information regarding *Mid* policies, procedures, processes or practices is also covered.

Network Administrator responsibilities

The Network Administrators will:

1. Maintain records of software licenses owned by *Mid*.
2. Periodically (at least annually) scan company computers to verify that only authorized software is installed. If unauthorized/unlicensed software is discovered it will be removed immediately.

Employee responsibilities

Employees:

1. Shall not install ANY software unless authorized by the Network Administrator. This includes screensavers and screen saver software. **Only software that is licensed to or owned by *Mid* is to be installed on *Mid* computers.**
2. Shall not copy software unless authorized by your Network Administrator.
3. Shall not download software unless authorized by your Network Administrator.
4. Shall sign applicable documents regarding confidentiality before being given access to computer and system.

Civil penalties

Violations of copyright law expose the company and the responsible employee(s) to the following civil penalties:

- Liability for damages suffered by the copyright owner
- Profits that are attributable to the copying
- Fines up to \$100,000 for each illegal copy

Criminal penalties

Violations of copyright law that are committed “willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b)),” expose the company and the employee(s) responsible to the following criminal penalties:

- Fines up to \$250,000 for each illegal copy
- Jail terms of up to five years