MARIETTA HOUSING AUTHORITY

INFORMATION TECHNOLOGY POLICY

1.0 Overview

Effective security is a team effort involving the participation and support of every MHA employee and affiliate who deals with information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

This policy is not to impose restrictions that are contrary to MHA's established culture of openness, trust and integrity. This policy was created to protect MHA, its employees and partners, from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Extranet-related systems, including computer equipment, software, operating systems, storage media, network accounts providing electronic mail and WWW browsing are the property of MHA. These systems are to be used for serving the interest of MHA.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at MHA. These rules and guidelines are in place to protect the employee and MHA. Inappropriate use exposes MHA to risks including virus attacks, compromise of network systems and servers, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at MHA. This policy also applies to equipment that is owned or leased by MHA.

4.0 Policy

4.1 General Use and Ownership

1. While MHA network administration desires to provide a reasonable level of privacy, users should be aware that data they create on the MHA systems remains the property of MHA. Because of the need to protect MHA's network, management cannot guarantee the confidentiality of information stored on any network device belonging to MHA.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use. If there is any uncertainty, employees should consult their supervisor or manager.
3. For security and network maintenance purposes, authorized individuals within MHA may monitor equipment, systems and network traffic at any time.
4. MHA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. User level passwords should be changed quarterly.
2. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic feature set to 10 minutes or less, or by logging-off (control-alt-delete) when the host will be unattended.

3. Postings by employees from a MHA email address to new groups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of MHA, unless posting is in the course or in the interest of MHA.
4. All computer systems used by MHA staff that is connected to the MHA network, whether owned by the employee or MHA, must be continually executing approved virus-scanning software with a current virus database.
5. MHA staff must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

4.3 Definitions

Blogging: a personal online journal that is frequently updated and intended for general public consumption.
Spam: Unauthorized and/or unsolicited electronic mass mailings.
Streaming: Multimedia that is continuously received by, and normally displayed to, the end-user while it is being delivered by the provider. The name refers to the delivery method of the medium rather than to the medium itself.

4.4 Unacceptable Use

Under no circumstances is an employee of MHA authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing MHA owned computer resources. (The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use).

4.4.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installations or distribution of "pirated" or other software products that are not appropriately licensed for use by MHA;
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and installation of any copyrighted software for which MHA or the end user does not have an active license;
3. Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses etc.);
4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home;
5. Using a MHA computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws;
6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not the intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. (For purpose of this section, "disruption": includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes);
7. Executing any form of network monitoring which will intercept data not intended for the employee's PC;
8. Circumventing user authentication or security of any host, network, or account;
9. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet;
10. Providing information about, or lists of MHA employees, to parties outside MHA.

4.4.2 Email and Communication Activities

The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam);
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of message;
3. Unauthorized use, or forging, of email header information;
4. Solicitations of email for any other email address other than that of the poster's account, with the intent to harass or to collect replies;
5. Creating or forwarding "chain letters", or other Pyramid schemes of any type;
6. Posting the same or similar non-business-related messages to large numbers of sent newsgroups (newsgroup spam).

4.4.3 Blogging

Blogging by employees, whether using MHA's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of MHA 's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate MHA's policy, is not detrimental to MHA's best interests, and does not interfere with en employee's regular work duties. Blogging from MHA's system is also subject to monitoring.

4.4.4 Streaming

Streaming music, video, talk show, or any other broadcasted material on the Internet is permitted, but MHA employees should limit streaming to periods when computer activity on the network is low.

5.0 Enforcement

Any employee found to have violated any policy set forth herein may be subject to disciplinary action, including termination.

6.0 Personal Mobile Devices

MHA employees with personal mobile phones and devices with email capability will receive high level support with regards to connecting to MHA email systems. The MHA IT Department will not support issues related to:

- Data connectivity
- Service interruptions
- Device support or training

7.0 User Access

The purpose of these procedures is to outline methods of securing MHA computing resources from unauthorized access. This policy and procedure document outlines the requirements for granting and terminating access to MHA information systems and resources and for determining appropriate level of access for employees, volunteers, business associates and representatives of entities doing business with MHA.

7.1 Policy

1. Access to MHA's information systems and resources is restricted to its own employees (Users) and in some cases, contract employees doing business on behalf of MHA.

2. The IT Manager can revoke authorization to access the MHA information system at any time if s/he suspects or detects that the individual is misusing information or information resources.
3. Authorized users are granted access to MHA information resources during scheduled work times, unless prior approvals have been granted by their immediate supervisor and a documented request given to the IT Department.

7.2 Access
1. Users' level of access to information systems is defined by their job descriptions and their need to access particular types of information in order to carry out the responsibilities of their position.
2. MHA department heads will complete and submit to the IT Department a written ***Request for Information System Access form*** asking that a User Name and Password be created or modified to gain or remove access to the MHA's system resources based on his/her positions.

7.3 Terminating Access
The IT Manager or a designated representative is responsible for terminating a user's access to the MHA's system in these circumstances:
- Evidence or reason to believe that the individual is using the MHA's information systems or resources in a manner inconsistent with Policy for Workstation Use.
- If the users password has been compromised and creates a thread to MHA's system resources.
- If the employee resigns or is terminated.
- If the employee's job description changes and the system access is no longer justified by the new job description.

8.0 <u>Password Administration and Configuration Requirements</u>

All employees and personnel who have access to organizational computer systems must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems. This policy applies to any and all personnel who have any form of computer account requiring a password on the organizational network including, but not limited to, a domain account and e-mail account.

8.1 Password Protection
1. Passwords should not be written down in place that is accessible by others.
2. Never send a password through email.
3. Never tell anyone your password, unless it is to gain access of your computer for a very short period of time; afterward your password should be changed.
4. Never reveal or hint at your password on a form on the internet.
5. Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
6. Never use your corporate or network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://
7. Report any suspicion of your password being broken to your IT department.
8. Don't use common acronyms as part of your password.
9. Don't use common words or reverse spelling of words in part of your password.
10. Don't use part of your login name in your password.
11. Don't use parts of numbers easily remembered such as phone numbers, social security numbers, etc.

8.4 Password Requirements
A Complex password contains both uppercase and lowercase letters and must contain a minimum of one number. The following password requirements has been set by IT Department:
- Minimum Length - 7 characters recommended

- Minimum complexity - No dictionary words included. Passwords should use three of four of the following four types of characters:

    - Lowercase
    - Uppercase
    - Numbers

- Passwords are case sensitive and the user name or login ID is not case sensitive.
- Maximum password age - 120 days
- Account lockout threshold - 3 failed login attempts
- Reset account lockout after - The time it takes between bad login attempts before the count of bad login attempts is cleared. The recommended value as of the date of writing this article is 10 minutes. This means if there are three bad attempts in 10 minutes, the account would be locked.
- Users should be in the habit of not leaving their computers unlocked, during extended time away from desk; they should use the CTRL-ALT-DEL keys and select "Lock Computer".

8.5 Enforcement

Since password security is critical to the security of the organization and everyone, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal.

9.0 Data Backup

This policy defines the backup policy for servers within the Marietta Housing Authority. Backup of systems typically refer to as servers, but are not limited to servers. Expected backup are file servers, mail server, and web server.

9.1 Definitions

Backup: The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
Archive: The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
Restore: The process of bringing offline storage data back from the offline media and putting it on an online storage system such as a file server.

9.2 Timing

Full backups are performed nightly on Monday through Sunday and incremental backup done every fifteen minutes.

9.3 Tape Storage and Data Retention

There shall be a separate or set of tapes for each backup performed on the Unix Server, including Monday through Friday. For all other servers located within the MHA's Data Room, full backups are located onsite and offsite in the event of a catastrophic system failure.

- The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed during a fifteen minute increment.
- Backup retention periods are for a minimal of two years or until the server meets its capacity, afterward the system will start overwriting based on the latest date.
- System backups are not meant for the following purposes:
    - Archiving data for future reference.
    - Maintaining a versioned history of data.

9.4 Testing
The ability to restore data from backups shall be tested at least once per month. The Yardi Live database should be copied to Test at least weekly.

9.5 Data Backed Up
Data to be backed up includes user data stored on the hard drive in the "My Document" directory. Systems to be backed up include but are not limited to:

- File server
- Mail server
- Production web server
- Production database server
- Domain controllers
- Test database server
- Test web server

9.6 Archives
User account data associated with the file and mail servers are archived one month after they have left the organization.

9.7 Restoration
Users who need files restored must submit a request to the help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

10.0 IT Department System Monitoring

The IT Department System Monitoring Policy defines the monitoring of MHA servers for both security and performance issues. This policy is designed both to protect the Marietta Housing Authority against loss of service by providing minimum requirements for monitoring servers. It provides for monitoring servers for file space and performance issues to prevent system failure or loss of service.

10.1 Scope
This policy applies to all production servers and infrastructure support servers including but not limited to the following types of servers:

- File Server
- Database Servers
- Exchange Server
- Application servers
- Report Server
- Domain controllers (DC1 and DC2)
- DNS Servers

10.2 Daily Checking
All servers shall be checked manually on a daily basis the following items shall be checked and recorded:

- The amount of free space on each drive shall be recorded in a server log.
- The system log shall be checked and any major errors shall be checked and recorded in the server log.
- Services shall be checked to determine whether any services have failed.
- The status of backup of files or system information for the server shall be checked daily.

10.3 Monitoring Resource Privilege and Rights
All Users group and login script should be checked on a bi-yearly basis to ensure system access is consistent with their job responsibilities.

10.4 External Checks
Essential servers shall be checked using either a separate computer from the ones being monitored or a server monitoring service. The external monitoring service shall have the ability to notify multiple personnel when a service is found to have failed. Servers to be monitored externally include:

- The mail server
- The web server
- External DNS servers
- Externally used application servers
- Database or file servers supporting externally used application servers or web servers

11.0 Incident Response and Escalation Plan

This incident response and escalation plan document discusses how information is passed to the appropriate personnel, assessment of the incident, minimizing damage and response strategy, and to access training needs within MHA.

11.1 Incident Definition
An incident is any one or more of the following:

- Loss of information confidentiality (data theft)
- Compromise of information integrity (damage to data or unauthorized modification).
- Theft of physical IT asset including computers, storage devices, printers, etc.
- Damage to physical IT assets including computers, storage devices, printers, etc.
- Denial of service.
- Misuse of services, information, or assets.
- Infection of systems by unauthorized or hostile software.
- An attempt at unauthorized access.
- Unauthorized changes to organizational hardware, software, or configuration.
- Reports of unusual system behavior.
- Responses to intrusion detection alarms through network tools.
- Compromised passwords.

11.2 Incident Detecting
When looking for signs of a security breach, some of the areas to look for in a network environment include the following:

- Accounting discrepancies
- Data modification and deletion
- Users complaining of poor system performance
- Large number of failed login attempts.

All incidents should be recorded on the ***Incident Notification Form*** and a summary of all incidents made available to management. All incidents should be reported to the IT Manager by phone, email or to helpdesk@mariettahousingauthority.org.

11.3 Analysis and Assessment

- Is the incident real or perceived?
- Is the incident still in progress?
- What systems are threatened and how critical is it?
- Is the incident inside or an outside source?

11.4 Response Strategy

- Is the response urgent?
- Can the incident be quickly contained?
- Will the response alert the attacker (Users) or do we care?

11.5 Containment

The containment process removes the infected or damage system from the network and the prevention steps provides steps to prevent re-infections.

- Disconnect the affected system(s).
- Change passwords.
- Block some ports or connections from some IP addresses.
- Close port on firewall.
- Shutdown infected system until it can be re-installed.
- Re-install the infected system and restore data from backup, prior to infections.
- Change email infecting the entire network.
- Make sure real time virus protection and intrusion detection is running.

11.6 Prevention and Monitoring

All efforts will be made to prevent security incidents by using the following measures:

- Clearly establish and enforce all policies and procedures.
- Gain management support for security policies and incident handling.
- Routinely assess vulnerabilities in your environment.
- Routinely check all computer systems and network devices to ensure that they have all of the latest patches installed.
- Develop, implement, and enforce a policy requiring strong passwords.
- Routinely check all logs and logging mechanisms, including operating system event logs, application specific logs and intrusion detection system logs.
- Verify your back-up and restore procedures.
- Making sure that you regularly verify backups and selectively restoring data.