Information Technology Acceptable Use Policy

Any questions related to this policy should be directed to the IT Director.

Overview

An Acceptable Use Policy is not intended to impose restrictions that are contrary to City of Hopkinsville's established culture of openness, trust, and integrity. The City of Hopkinsville Information Technology division (COHIT) is committed to protecting city's employees, partners, and the city from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP are the property of City of Hopkinsville. These systems are to be used for business purposes in serving the interests of the city in the course of normal operations. Please review Human Resources policies for further details.

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

Policy and Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at the City of Hopkinsville. These rules are in place to protect the employee and the city. The City of Hopkinsville prohibits the inappropriate use of any device that exposes the city to risks including virus attacks, compromise of network systems and services, and/or legal issues.

This policy applies to the use of information, electronic and computing devices, and network resources to conduct City of Hopkinsville business or interact with internal networks and information systems, whether owned or leased by the City of Hopkinsville, the employee, volunteer, or a third party. All employees, contractors, consultants, temporary and other workers at the City of Hopkinsville or its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the City of Hopkinsville's policies, standards, and local laws and regulation.

Responsibility for Compliance:

- All employees, volunteers, and appointed positions.
- Workers whose job functions fall within the scope of this policy by virtue of the types of data access which they are granted, either explicitly or implicitly (such as access to network shares or documents containing data covered by the scope of this policy).

- All contractors, vendors, and any other third parties entrusted with sensitive, confidential, or highly confidential city data.

Policy

General Use and Ownership

- City of Hopkinsville proprietary information stored on electronic and computing devices whether owned or leased by the city, the employee, or a third party remains the sole property of City of Hopkinsville. You must ensure through legal or technical means that proprietary information is protected in accordance with other city policies.
- You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of the City of Hopkinsville's proprietary information to the IT Director (pursuant to KRS 61.932 and the city's Protection of Personal Information Policy).
- You may access, use, or share City of Hopkinsville proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use; if there is any uncertainty, employees should consult with their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within the City of Hopkinsville may monitor equipment, systems, and network traffic at any time.
- City of Hopkinsville reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

- System-level and user-level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure access, is prohibited.
- All computing devices must be secured with a password-protected lock screen with the automatic activation feature set. You must lock the screen or log off when the device is unattended for an extended amount of time.
- Postings by employees from a City of Hopkinsville email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of City of Hopkinsville, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, as they may contain malware.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the City of Hopkinsville authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing the City of Hopkinsville-owned 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.

System and Network Activities

The following activities are prohibited:

- Violations of the rights of any person or protected entity by copyright, trade secret, patent, or other intellectual property or similar laws or regulations including but not limited to the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by City of Hopkinsville.
- Unauthorized copying of copyrighted material including but not limited to digitization and distribution of photographs from magazines, books, other copyrighted sources, or copyrighted music
- The installation of any copyrighted software for which City of Hopkinsville or the end user does not have an active license.
- Accessing data, a server, or an account for any purpose other than conducting City of Hopkinsville business.
- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws. This is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Allowing someone else to use your computer with your user id. If needed for support, you must monitor actions that are being done under your user logon session.
- Using a City of Hopkinsville computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace policies.
- Installing remote access software without COHIT advance knowledge and approval.
- Connecting any equipment that is not owned by the City of Hopkinsville's internal network. The only city network that will allow outside equipment connections will be labeled "City-Public"; connections to this network may be wired or wireless. Please contact the COHIT team with help on this matter.
- Making fraudulent offers of products, items, or services originating from any City of Hopkinsville account.
- Effecting security breaches or disruptions of network communication. Security breaches include but are not limited to accessing data of which the employee is not an 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 purposes 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.
- Port scanning or security scanning is expressly prohibited unless prior notification to COHIT is made.

- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Introducing honeypots, honeynets, or similar technology on the City of Hopkinsville network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- 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/Intranet/ Extranet.

Email and Communication Activities

The following activities are prohibited:

- 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).
- Any form of harassment via email, telephone, or paging whether through language, frequency, or size of messages.
- Unauthorized use or forging of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within City of Hopkinsville's networks of other Internet/Intranet/Extranet service providers on behalf of or to advertise any service hosted by City of Hopkinsville or connected via City of Hopkinsville's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Social Media Activities

All persons covered by this policy will strictly follow the following guidelines, without exception:

- Social media activities by employees or volunteers, whether using City of Hopkinsville’s property and systems or personal computer systems, are also subject to the terms and restrictions set forth in this policy. Limited and occasional use of City of Hopkinsville’s systems to engage in social media activities is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate a City of Hopkinsville policy, is not detrimental to City of Hopkinsville’s best interests, and does not interfere with an employee's regular work duties. Social media activities conducted from City of Hopkinsville systems are also subject to monitoring.
- City of Hopkinsville’s Protection of Personal Information Policy also applies to social media activities. As such, employees and interns are prohibited from revealing any City of Hopkinsville confidential or proprietary information, trade secrets, or any other material covered by said policy when engaged in social media activities.

- No employees or interns shall engage in any social media activities that may harm or tarnish the image, reputation, and/or goodwill of the City of Hopkinsville and/or any of its employees. Employees and interns are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when engaging in social media activities or otherwise engaging in any conduct prohibited by City of Hopkinsville's Employee Policies and Procedures Handbook.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, City of Hopkinsville's trademarks, logos, and any other City of Hopkinsville intellectual property also shall not be used in connection with any social media activities unless done as part of an employee's specific job function.

Policy Compliance

Compliance Measurement

- The COHIT team will verify compliance to this policy through various methods including but not limited to business tool reports, internal and external audits, and feedback to City Administration.

Exceptions

- Any exception to the policy must be approved by the COHIT team and department heads in advance.