INFORMATION TECHNOLOGY AND COMMUNICATION COMMITTEE MEETING

WEDNESDAY, MARCH 4, 2020
4:00 P.M.
MINUTES

MEMBERS PRESENT: Commissioners Brandon Haskell, Rob Piercefield, Brian Droscha, Brian Lautzenheiser, Jeanne Pearl-Wright and Wayne Ridge

MEMBER ABSENT: Commissioner Jane Whitacre

ALSO PRESENT: Commissioner Terrance Augustine; Jeff Parshall and Connie Sobie

The March 4, 2020 regular meeting of the Information Technology and Communication Committee was called to order at 4:00 p.m. by Chairperson Haskell.

The Pledge of Allegiance was given by all.

Commissioner Ridge moved to approve the agenda, as presented. Commissioner Lautzenheiser seconded. Motion carried.

Commissioner Droscha moved to approve the minutes of the January 8, 2020 meeting, as presented. Commissioner Pearl-Wright seconded. Motion carried.

The acceptable use policy and updated user access policy was presented. Jeff Parshall provided an update on the user access policy. Discussion held.

Commissioner Droscha moved to recommend approval of the Acceptable Use Policy and User Access Policy to the Board of Commissioners. Commissioner Lautzenheiser seconded. Motion carried.

An update was provided on the following technology projects: The GIS aerial flyover, infrastructure project, Parks and Recreation Civic Rec site for on-line scheduling and credit card acceptance, dash cam equipment being replace with cloud based unlimited data access, Office 365 transition, Dropbox changes, courtroom technology projects and ADA compliance of courtroom technology.

Chairperson Haskell adjourned the meeting at 4:45 p.m.

The next regular meeting of the Information Technology and Communication Committee will be held on Wednesday, April 1, 2020 at 4:00 p.m. in the Board of Commissioners Room of the courthouse located at 1045 Independence Boulevard, Charlotte, MI 48813.

Brandon Haskell, Chairperson

Acceptable Use Policy

1.0 Overview

This Acceptable Use Policy demonstrates a commitment to protecting the county's technology assets and access to digital data that is collected, stored, analyzed, and reported upon by employees throughout the county.

County computer networks, including all host and server systems, locally or externally operated, are the property of Eaton County. These systems are to be used for business purposes in serving the interests of the county in the course of its business operations.

Effectively securing our technology assets and digital data is an obligation of every employee who uses any component parts of the computer network. Therefore, employees must understand the impacts these guidelines have on their use of network and standalone resources.

2.0 Purpose

The purpose of this policy is to broadly outline acceptable use of any and all computer networks and individualized systems like personal computers, laptops, and mobile devices. Inappropriate use exposes both the county and the employee to risks that include disruptions in work processes resulting from computer viruses and other malicious software. Additional concerns include unauthorized access to, and/or the transfer of, digital data and identify theft.

This policy shall be influenced by the requirements of the most current version of the ***Michigan Criminal Justice Information System Guidelines*** that mandate certain requirements as they relate to LEIN/NCIC. Periodic updates to this policy may be determined by these guidelines.

3.0 Scope

This policy applies to all employees and all technology assets (servers, PCs, laptops, mobile devices, and so on) that are owned or leased by the county.

4.0 Policy

4.1 General Use and Ownership

1. Digital data created and stored in any computer system is the property of the county. Employees shall not copy or otherwise transfer files created during the course of their employment to a personally owned fixed or removable storage device, Internet-based storage service (i.e., cloud storage) without approval from the highest ranking elected or appointed official responsible for administration and oversight of the digital data's use, storage, analysis and reporting.

2. Digital data files, including databases, word-processing files, spreadsheet files, and similar universally accepted file formats, created during the course of an employee's official duties, shall be stored on the county's computer network to ensure protection, retention, and ongoing access to the files. "Convenience copies" of data may be stored on various media and/or locations following the requirements of item #1 above.
3. The Director of Information Systems, or designee, shall regularly monitor and evaluate use and security of all component systems that make up the entire county network and shall do so in accordance with the previously adopted **Audit Policy**. Networks and systems may be audited on a regular basis to ensure compliance with this and other information technology policies adopted by the Board of Commissioners.

4.2 Security and Proprietary Information

1. Employees should take all necessary steps to prevent unauthorized access to county digital data by anyone not authorized to access the data.
2. Keep network and system login credentials (user Id and password) secure and do not share this information with anyone lacking authorization (i.e., an employee in a department not related to your own). Employees are required to periodically change their password(s). See the county's ***Password Policy*** for more information.
3. Employees are required to logoff from or otherwise lock their personal computer, laptop, or mobile device when not in use.
4. Because information contained on laptops and other mobile devices is especially vulnerable to loss, special care should be exercised when using these systems when working from remote locations. If a device is lost or stolen it must be immediately reported to the Information Systems Department.
5. All network servers, personal computers, laptops, and related devices shall continually execute an approved virus protection program. Because these programs cannot guarantee the presence of a virus, employees shall continually exercise caution when sharing files, downloading files, connecting to the Internet, and other service-oriented sites.
6. Employees shall not use their county e-mail account for a non-county enterprise (such as Barnes and Noble, Groupon, Facebook, and many other enterprises) unless it is explicitly related to their job responsibilities as defined and approved by their supervisor. See the county's ***Password Policy*** for more information.

4.3. Unacceptable Use

The following activities are prohibited. Employees may be exempted from these restrictions as approved by the Board of Commissioners, County Controller, Director of Information Systems or other authority. However, no exemption shall be allowed if one or more parties can show the exemption would be detrimental to the operational "welfare" of the county's computer network.

The lists below are by no means exhaustive. Rather, they attempt to provide a framework for activities which fall into the category of unacceptable use.

General

1. Under no circumstances is an employee authorized to engage in any activity that is illegal (under local, state, federal or international law) or deemed to be inappropriate or immoral by the Board of Commissioners.

Technical

1. Violations of the rights of any person or organization protected 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 Eaton County. See also the ***Resolution to Comply with Software Licensing Agreements to Ensure Legal Software Use***.
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 the installation of any copyrighted software for which the county or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Appropriate management should be consulted prior to exporting any material that is in question.
4. Introduction of malicious programs into the network, servers, personal computers, laptops, mobile devices, and related devices.
5. Allowing use of your network account and/or password by other individuals not specifically authorized by the employee's supervisor to use the account.
6. Using a computer to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
7. Making fraudulent offers of products, items, or services originating from any county e-mail account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions (such as denial of service) of network, servers, personal computers, laptops, and mobile devices. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a computer that the employee is not expressly authorized to access.
10. Port scanning or security scanning is expressly prohibited unless prior notification to the county is made and the Director of Information Systems authorizes such scanning to occur.

11. Executing any form of network monitoring which will intercept data not intended for the employee's host or server system, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any network or system access account.
13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, an employee's computer system.
14. Sending unsolicited e-mail messages, including the sending of "junk mail" and "chain letters" or other advertising material to individuals who did not specifically request such material (this is e-mail spamming).
15. Any form of harassment via e-mail, telephone or paging, whether through the use of language, frequency of occurrence, or size of messages.
16. Unauthorized use, or forging, of e-mail header information.

See the ***Electronic Mail Policy*** for additional information.

4.0 Enforcement

Employees found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	**Definition**
Spam[ming]	Unauthorized and/or unsolicited electronic mass mailings.
LEIN	Law Enforcement Information Network
NCIC	National Crime Information Center

7.0 Revision History

This policy update supersedes the Acceptable Use Policy previously adopted by the Board of Commissioners on 12/2/2011.

Information Security Policy Manual - User Access Policy

Abstract

This Information Security Policy Manual (ISPM) provides guidance for the creation, deletion and maintenance of network user access accounts.

Version Number	1.5
Last Revision Date	02/25/2020
Document Reference	ISPM12UAP
Classification	Internal use only

REVISION HISTORY

**Updates to this table must be made at each revision of this policy*.

DATE	AMENDED BY	APPROVED BY	SIGNATURE	DESCRIPTION
07/26/19	AI Security Team			Initial Draft
09/09/2019	AI Security Team			Integrated Eaton County policies – Computer Access and Security Policy, Enhanced Access to Public Records Policy (Exemption Revision), Enhanced Access to Public Records Policy and Internet Use Policy - December 2000.
09/17/2019	Eric P. Daley			Department name update. Revise review schedule. Remove Enhanced Access to Public Records and Internet Use Policy sections of draft policy.
02/25/2020	Jeff Parshall			Add identification and signature lines as required by Pub 1075 standards.

TABLE OF CONTENTS

1. OVERVIEW

Eaton County, hereinafter referred to as County, provides network user accounts to all employees, contractors and part time employees that access information on the County network. Accounts issued are for County use only.

County provides a number of computer systems to employees for performing their respective business functions. Each computer system, accessible to employees, requires that an employee use a unique user name and password when accessing these computers. This requirement is consistent with mandates found in the **Michigan Criminal Justice Information System Guidelines as they relate to LEIN/NCIC as well as Internal Revenue Service Publication 1075 (IRS Pub 1075) Guidelines**.

2. PURPOSE

The purpose of this procedure is to provide a policy and guideline for creating, modifying, or removing access to County's network and data by creating, changing or deleting the network account configuration for a User. In addition, to ensure that employees do not share their user name and/or password with anyone inside or outside of the county.

3. SCOPE

This policy and defined process is used to allow access to County's data and systems to individuals who meet the requirements defined in this policy. This policy governs all individuals who are granted access that is necessary to support the business. This policy relates to all data used, processed, stored, maintained or transmitted in and through County systems.

4. POLICY

Access to network resources (i.e., email, applications, files shares, etc.) will be granted after proper paperwork has been submitted and approved. Each user will be issued his/her own unique account to access network resources. User accounts shall not be shared. Users shall not use generic accounts unless the account is required for a business reason, documented and approved by Management. Users will be responsible for maintaining a strong password on their account to prevent possible misuse of their account.

Sharing user names and passwords allows other individuals to access vital, sensitive, or confidential County information. It also allows a person the opportunity to "simulate" or "pretend" to be someone they are not while using a computer system. Such activities shall be avoided in compliance with county requirements and/or Michigan Criminal Justice Information System Guidelines as they relate to LEIN/NCIC as well as Internal Revenue Service Publication 1075 (IRS Pub 1075) Guidelines.

4.1. ACCOUNT MANAGEMENT

All user accounts will be actively managed by the County Technology Services Network Administrators. Active management includes the responsibility to establishing new user accounts, activate and certify, modify, disable, and audit user accounts in the County system. User account changes are to be requested by the user's direct manager or another employee who has been provided the authorization to do so as part of their required job functions. At the time of termination all user access to network must be immediately revoked and disabled. Users who performed privileged functions (e.g., system administration) must use separate accounts when performing those privileged functions. All users who perform account management functions are prohibited from modifying or altering any accounts or privileges related to an account they currently control or use.

All vendor accounts will be actively managed by the County Technology Services Network Administrators. All vendor account must be clearly identified and differ from standard employee user accounts. Active management includes the responsibility to establishing vendor user accounts, activate and certify, modify, disable, and audit user accounts in the County system. User account changes are to be requested by the user's direct manager or another employee who has been provided the authorization to do so as part of their required job functions. At the time of termination all user access to network must be immediately revoked and disabled.

All access to user management systems that centrally manage user access to physical and logical security are accessed by authorized personnel. User management systems must be securely stored, managed and accessed only by authorized personnel. All authorized personnel must be approved by management.

4.2. PRIVILEGES

User accounts are to be constructed such that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with that account. User accounts are only to have the minimum access required to perform tasks associated with that users account. Any privileges or access to data outside of the requesting manager's ownership needs to be approved by the data's respective owner prior to implementation. All remote access sessions must be authorized, encrypted and provide additional reasonable measures of security where possible.

4.3. ACCOUNT REVIEW

User accounts will be reviewed to identify accounts with inappropriate privileges (either too high or too low), as specified by Michigan Criminal Justice Information System Guidelines as they relate to LEIN/NCIC as well as Internal Revenue Service Publication 1075 (IRS Pub 1075) Guidelines. Should accounts be discovered with inappropriate privileges those privileges will be reset to the established level for the user's responsibilities. Should the account continue to remain inactive for 2 months it should be manually disabled. All administrative and inactive accounts will be reviewed on a bi-monthly basis by Technology Services and approved by department manager.

5. ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and possible criminal charges. Violations of this policy will be submitted to the offending employee's Department Head and County Controller for review and/or resolution. As it relates to the

courts, the violation shall be reported to the Chief Judge.

6. DEFINITIONS

LEIN - Law Enforcement Information Network

NCIC - National Crime Information Center

Software - means that term as defined in section 2 of the Enhanced Access to Public Records Act, Act 462 of the Public Acts of 1996.

7. REFERENCES

None

Each users that accesses the Eaton County Network must fill out the following user information and sign this document to be allowed to access the Eaton County Network and applications:

Printed Name_____

Organization/Department: _____ Date: _____

Signature: _____

The signed copy of this policy must be provided to Eaton County Technology Services before access to the County Network will be allowed.