Winona County

Acceptable Use Policy for Electronic Communications and Internet Use Policy 6.50

Board Approval Date: 09-23-2008 Supersedes Policy Dated: 07-13-1999

Policy

Winona County recognizes that phone and computer systems are becoming increasingly interconnected and sophisticated in their ability to create, disseminate, and store electronic messages, along with an increased potential for the inappropriate release of non-public data.

Winona County has developed policies and guidelines regarding the use of all electronic communications systems and information transmitted through or stored in those systems.

This policy applies to all Winona County system users regardless of location, status, or ownership. Each system user is responsible for adhering to the guidelines and policies regarding the use of these systems to protect the accuracy, integrity, and dependability of the organization's electronic systems and information.

The computer and communications systems operated by the employees for the conduct of business are the property and work environment of Winona County, and all Winona County policies relating to personal conduct apply to access and use of these resources.

Users have no expectation of privacy in using these systems. No communication using these systems should be considered private or personal. Records retention policies apply to electronic communications, users should assume that even deleted messages are retrievable at a later date.

Winona County can and will inspect information stored in or transmitted through its electronic systems.

Winona County provides telephone, fax, internet access, and e-mail to speedily conduct the business of the organization. Use of these systems will be granted by supervisors with regard to job function. Once given access, users are expected to use these systems in a responsible manner at all times. All usage should be able to withstand public scrutiny without embarrassment to Winona County.

The Winona County Electronic Mail System (e-mail) is designed to facilitate County business communication among employees and other business associates for messages or memoranda. Since no computer system is completely secure, the e-mail system is not intended to transmit sensitive materials, which may be more appropriately communicated by written memorandum or personal conversation.

System users are responsible for the content of all text, audio, and video sent using the Internet or phone systems. All messages must comply with relevant Federal and State laws regarding copyright, trademark, and intellectual property. Messages must contain the user's identity, and should be written with the same professional manner as any hard-copy correspondence.

System users are not allowed to release passwords or user names, to anyone other than designated individuals. Designated individuals will be established by the department head and/or supervisor.

System users cannot access or modify any information without the express prior permission of the authority responsible for generating or maintaining said information.

Winona County's policies pertaining to harassment and other forms of workplace misconduct apply with full force and effect to the use of Winona County's electronic communication systems.

Personal, non-work related use of telephone, fax, Internet access, and e-mail is permitted, provided such use

1) does not impair the employee's workplace performance and productivity;
2) is done on the employee's personal time;
3) does not interfere with business usage;
4) does not contain harassing or threatening material;
5) is not performing work for profit, for personal gain, promotional use or solicitation;
6) does not contain abusive, profane, or offensive language/content;
7) does not interfere with other employees' job activities;
8) is not for political, religious, personal financial profit, or other promotional activities, or does not result in consumption of County resources;
9) does not result in incremental expense for the County;

(Note: Winona County can prohibit the use of any/all of this equipment or set limitations on its usage).

The use of Winona County's electronic communication devices is a privilege, not a right, which may be revoked at any time.

Internet

The Internet provides Winona County with significant access and dissemination of information to individuals outside of Winona County. The use of the Internet system, via County computers, is intended to serve County business. The system is not to be used for employee personal gain or to support or advocate for non-county related business or purposes. Like all e-mail messages, Internet messages are capable of being forwarded without the express permission of the original author. Therefore, users must use caution in the transmission and dissemination of messages outside of the County, and must comply with all State and Federal laws.

Inappropriate use of telephone, fax, Internet access, and e-mail systems would include but are not limited to participation in illegal activities, gambling, commercial activities, accessing sexually explicit or violent material; using the systems to harass or disable other systems, creation or distribution of virus or destructive programs, distributing pirated software or stolen data or any other activity that injures others or Winona County in any way.

Requests for information can become very time-consuming and expensive. Winona County may maintain public access points for information, and access to Winona County records. These systems should be operated only by persons specifically authorized (and trained) to place or remove data on such a system. Release of data to the public in other formats should be carried out through authorized channels.

Incoming messages containing file attachments may imperil Winona County systems by importing viruses. Files or mail attachments entering Winona County's network should always be scanned for viruses before being opened or used.

It is the department head/supervisors responsibility to oversee use and to determine if uses of electronic systems are appropriate to assigned work. Although content is not routinely monitored, it may occur internally under administrative procedures, and externally under subpoena, request for public data or other legal actions, or due to unexpected absence of an employee, or for other business or technical reasons.

Retention of E-Mail

Generally, e-mail messages are temporary communication, which are non-vital and may be discarded routinely. However, depending on the content of the e-mail message, it may be considered a more formal record and should be retained pursuant to a department's record retention schedule. Examples of messages of this nature are: policy, decision making, connected to specific case files, contract related or otherwise an essential part of a larger record, or other memorandum of significant public business. As such, these e-mail messages are similar to printed communication and should be written with the same care. Each department head/supervisor is responsible for establishing and maintaining department retention schedules for the information communicated through the e-mail system.

Winona County reserves the right to treat the misuse of these resources as any other act of employment in accord with its personnel policies and procedures. Violations of this policy will subject the user to discipline, up to and including discharge as well as notification to law enforcement agencies when appropriate.

I acknowledge that I have read the above policy regarding the use of electronic systems of Winona County.

____ ____________________

User's Signature and Printed Name Date

I acknowledge that I have made this Policy regarding the use of electronic systems available to the above-named person for review.

____ ____________________

Department Head/Supervisor's Signature and Printed Name Date

WINONA COUNTY

SECURITY GUIDELINES

Approved by County Board: 09/23/08

1. Purpose

These Security Guidelines describe how Winona County Staff should handle information resources in order to help ensure the confidentiality, integrity and availability of all Winona County governmental-related and operational information. These Guidelines apply to **all individuals** who are authorized to use the information resources of Winona County, including Winona County employees, support staff, administrators, volunteers, board members, designees, contractors, elected and appointed officials, interns, and members of the general public.

2. Introduction

These Security Guidelines are based on an analysis of the information assets, requirements and risks associated with information and information systems at Winona County. These Guidelines provide a reference for protecting all information in all Winona County information systems.

These Guidelines apply to all information resources that the County owns and controls. Such systems and information assets included (but are not limited to) telephone systems, computer systems and networks, printers, voicemail systems, cellular phones, pagers, facsimile machines, electronic mail systems and messaging systems, and connected electronic networks.

The overall County security objective is to ensure the confidentiality, integrity, availability and safety of all Winona County-related information. These Guidelines support that objective by including statements that are designed to minimize the effect of the threats and vulnerabilities on information systems. These Guidelines address four critical security objectives within Winona County.

- Confidentiality Objective
  All data should be protected from unauthorized disclosure. Non-public data should remain as private as possible. Release of this data will only be to properly authorized individuals and entities.

- Integrity Objective
  All data shall be protected from improper or unauthorized creation, modification or destruction. Data should be created and entered correctly, and modified by only those individuals who are authorized to do so.

- Availability Objective
  All Winona County authorized users shall have unhindered access to the data they require to perform their authorized tasks. Winona County is committed to minimize and mitigate the chance of a catastrophic failure through these policies. Included in this commitment is the development of a comprehensive disaster recovery plan for the County.

- Safety Objective
  Winona County is committed to protecting county assets and authorized users.

3. Authorized Uses

Winona County's Electronic Communications Systems are for use by Winona County authorized users. Acceptable uses of Winona County's Electronic Communications Systems are described in the Winona County Acceptable Use Policy *Strictly personal use of Winona County's Electronic Communications Systems may occur as long as such use is of negligible impact and* *incidental in nature*. Employees are not permitted to use Winona County's Electronic Communications Systems for personal commercial purposes, nor for any illegal purposes.

3.1 Allocation of Resources

Appropriate personnel and financial resources should be made available to information system staff to ensure that adequate security methods and user training are provided and maintained.

3.2 Acceptable Use Policy and Guidelines

Winona County will publish and distribute the Acceptable Use Policy and Guidelines to authorized users and provide financial resources to ensure that adequate user training is provided.

4. Access Control

Access to Winona County facilities, computer systems and other technology resources should be strictly controlled so that only Winona County authorized users have access to the available information. So, for example, access to Internet resources will be granted based on a need to perform authorized job functions. Public access to public data (as defined by Minnesota statutes) must be maintained without compromise to the overall integrity of recordkeeping systems and maintenance procedures. At the time of this writing of these Guidelines, the County may charge reasonable fees for access to public data, including the costs to compile, maintain and furnish public data.

4.1 Access Control Mechanisms

The base level of access to Winona County networks and information systems is based on the privileges and requirements needed to perform work functions, and some form of Access Control Mechanism should control all accesses to sensitive, private, copyrighted, or licensed information.

The mechanism (such as keys, passwords, picture and/or magnetic strip ID badges, or tokens like Smart Cards) used to verify accesses should be protected at the same level that staff would protect any information on the system, or in the physical area to which the Access Control Mechanism grants them access. For one common example, passwords should not be written on sticky-notes and pasted to the side of the computer if access to this computer is controlled to prevent unauthorized access.

Loss or suspected loss of the Access Control Mechanism should be immediately reported to the Information Technology Director.

4.1.1 Password Policies

Passwords used within Winona County Information Systems will be single user, non-repetitive passwords that have no direct relationship to the password user and/or creator, and which periodically expire.

Training in proper password selection, protection, and in administration password policies should be conducted with all new employees during orientation and reviewed periodically by each department to ensure a common Winona County standard.

4.1.1.1 Password Sharing

Passwords should not be shared across multiple users, or across multiple computer systems, unless expressly approved by the Information Technology Director.

4.1.1.2 Password Expiration

Passwords will be changed periodically as determined by the password policy for each system—in general this will be every 90 days. On automated systems with the capability, users should receive prior notice that their password is about to expire so that they are provided ample opportunity to change their password.

4.1.1.3 Password Complexity

Passwords used should be of sufficient complexity that they are not easily guessed. This includes such characteristics as:

- Passwords should use at least five (8) alphanumeric characters.

- Passwords should not be obviously related to the user. This includes such items as spouse, children, or pet names or nicknames, license numbers, or phone numbers.

- Good passwords can be created using the first initials of a sentence, using capitalization and punctuation.

4.1.1.4 Password Protection

Winona County users should protect their passwords from any and all other individuals, and users should also respect this requirement on co-workers.

This guideline is intended to include such items as:

- Disclosure of a Winona County user's password to any person other than the password's owner is prohibited.

- A Winona County user should not enter his or her password if someone else is watching.

- Winona County users should not watch any other Winona County user enter their password.

- Passwords should not be written down in any readable form, or programmed into any computer system or key for automatic login, recall, display or other use, except for a controlled password registry.

4.1.1.5 Administrator Password

Administrator passwords will not be shared, and will be changed with greater frequency than that required by these Guidelines, to ensure the confidentiality of administrator accounts. Administrator level accounts clearly marked (e.g. ADMIN_LAURA) should only be used when performing duties requiring administrative access. Administrators should return to a "normal user" level when not performing administrative duties.

4.1.1.6 Training Passwords

Passwords created for training purposes should be changed regularly and should be restricted to access from systems designated as training resources. All training systems should have passwords. Training passwords should be activated only when training is in session.

PASSWORD REGISTRY

Persons with responsibility for system administration should record access passwords in a confidential password registry, to be maintained by IT. Inability to access critical systems could cause major denial of service and result in unacceptable downtime for information systems.

Name of Computer System
Make, Model of CPU
Location Building Room # Location in Room
Supervisor/Root/Administrator Username Other Relevant Information Supervisor/Root/Administrator Password
Support Contracts Vendor furnishing support date support begins
Phone, contact date support ends
Next escalation step (if known) after local support
Vendor Contacts Purchased from date purchased
Special terms and conditions of purchase
Back-Ups Normal back-up method LAN Tape Floppy Incremental Full
Location of on-site and off-site backups
Name of Person Completing this Form Phone: Work Home Pager

Thank you for your help in making our information systems more dependable.

4.1.1.7 Suspected Disclosure

In event of a suspected disclosure of a password, that password should be immediately changed.

4.1.2 Password Registry

Persons with responsibility for system administration will record access passwords in a confidential password registry, to be maintained by the Information Technology Director. The registry should also contain information about support contracts, vendor contacts, and location of on-site and off-site backups. Access to this Registry should be controlled with extreme vigilance.

Failure to document updates to critical systems could cause major denial of services and result in unacceptable downtime for information systems.

Systems to be included in the password registry include telephone systems, security systems, workstations with significant amounts of data stored locally, networking systems, and file servers.

4.2 Login Banner

Every login screen on every computer system should contain explicit statements that include the following ideas:

- access to the system is for authorized users only;

- by accessing the system, the user is representing that they are an appropriately authorized user;

- by accessing the system, the user is agreeing unconditionally to be covered by the rules and regulations of Winona County.

- That violation of the rules and regulations of Winona County and these Security Guidelines is subject to disciplinary action and/or criminal prosecution.

Example:

> Access to this system is for Winona County authorized individuals only. By accessing this system, you acknowledge that you are such an individual, and that you will abide by all Winona County rules, regulations and policies. Violators will be subject to disciplinary action and/or criminal prosecution.
>
> For assistance, call the Information Technology Department at extension 6330.

5. Security Awareness / User Responsibilities

5.1 Disclosure of Information

Winona County authorized users are NOT authorized to disclose any Winona County private data on individuals, confidential data on individuals, and nonpublic data to former Winona County employees, or to other non-Winona County individuals, unless provided with prior written authorization.

5.2 User Training

Winona County authorized users should receive periodic training by department heads or supervisors to ensure that relevant issues in these guidelines are addressed.

5.3 Logout Unattended Terminal/System

Winona County authorized users should logout of computer terminals or systems if they are going to leave the computer terminal system unattended. Automatic logouts or password-protected screensavers should be enabled wherever practical.

5.4 Alert Computer Use

Winona County staff should be alerted about their computer or terminal status and take care that unauthorized individuals cannot read or modify data through a valid system login or session. Low-tech solutions can include anti-glare screen guards that prevent *"shoulder surfing"* and proper monitor placement.

Note: The intent of this guideline is for a user to be aware that potentially sensitive data may be displayed on a computer screen they are using. Users should take appropriate steps to ensure that unauthorized people are not reading over their shoulders.

5.5 Alert Printer Use

When a user prints sensitive, proprietary or otherwise controlled information, that user should retrieve the printed material in a timely manner to ensure that it is not available for unauthorized use.

5.6 Responsible Information Use

Winona County staff should not make extra copies of any Winona County or client information beyond what is required to perform official duties.

5.7 Personal Privacy Zone

Winona County authorized users should make an effort to teach appropriate privacy behaviors concerning password entry as a part of general "nettiquette."

6. System Management

6.1 System Administration

Winona County should designate staff to perform system administration and user account functions for each system. Such individuals have a great deal of access to sensitive information resources, and their work habits may be monitored more closely than average employees.

6.1.1 System Administrator Account

System administrators will use system administrator accounts to perform system administration and user account maintenance functions only. These individuals will use regular accounts for non-administrator functions.

6.1.2 System Administrator Rights and Responsibilities

System administrators have the right and the obligation to take necessary actions to ensure the availability of the computer system that they are supporting.

6.1.3 IT to be Notified of User Status Changes

Supervisors and Personnel Department staff must communicate with IT to manage access to all electronic systems.

Any change in a Winona County professional's status that could involve restriction or termination of information system permissions should be immediately communicated by the appropriate supervisor to the Information Technology Director. This includes changes in the status of temporary staff, leave of absence, resignation, and extended sick leave or vacation.

The Information Technology Director will notify the system administrators to deactivate or transfer the user accounts. Information about staff replacements are very helpful in making a smooth transfer of privileges.

Note: Inactive accounts are often a primary target for attempted unauthorized access. When a Winona County staff member is dismissed or terminated involuntarily, all computer and information system permissions, User IDs and passwords should be disabled prior to notification of the employee.

6.1.4 Terminated Employees

Persons not actively employed by the County will not have access to computer networks, e-mail, dial-up services, voicemail, or other electronic communication systems.

When a Winona County staff member is dismissed or terminated involuntarily, all computer and information system permissions, User IDs and passwords should be disabled prior to notification of the employee. Further, other staff members should be fully informed that they are in no way to provide the individual with any access to any Winona County information processing system.

The overall goal of the following sections is to eliminate and pass around the duties and responsibilities within 30 days.

6.1.4.1 Voicemail

Voicemail stored on the system will be saved and access given to the supervisor for disposition and routing of existing messages.

□ Voicemail access given to the supervisor. Access password_________________.

□ Disposition of existing messages completed. ________________________(date)

6.1.4.2 Internal E-mail

Internal e-mail will be disabled immediately. As soon as practical, the former employee's name should be removed from the e-mail lists it was in. If there is a gateway between the employee's internal and internet mail it should be disabled immediately as well, to prevent internal mail from "leaking" into the Internet mailbox where it could be accessed.

□ Internal e-mail disabled. _______________________ (date)

□ Name removed from the e-mail directory and lists. ____________________(date)

□ Gateway between internal and internet mail disabled. __________________(date)

6.1.4.3 Internet E-mail

Internet mail directed to a former employee should be forwarded to the employee's supervisor for disposition. In addition, Winona County may (but is not obliged to) send an auto-reply to the sender informing them of the employee's absence. One option the supervisor has is to forward messages of an obvious personal nature to the former employee, but this is not a requirement of these Guidelines.

□ Internet mail forwarded to the employee's supervisor. ________________________(date)
□ Auto-reply informing senders of the employee's absence.(Optional)______________ (date)

6.1.4.4 Remote Network Access

Network access, including direct access from the LAN and remote network access, either through dial-up or through the Internet into the Winona County administrative networks, shall be stopped, at the latest, on the employee's termination of employment. Network administration requirements may be such that certain accesses need to be curtailed earlier.

□ Network access stopped. __________________(date)

□ Remote network access stopped. __________________(date)

(Note: Network administration requirements may be such that certain accesses need to be curtailed earlier than the employee's last day of employment.)

6.1.4.5 Administrative Passwords

Override and common administrative passwords must all be cycled whenever an individual who had knowledge of these passwords terminates employment.

□ Override passwords changed. ___________________(date)

□ Common administrative passwords changed. ___________________(date)

6.2 Configuration Management Policies

Winona County will perform regular configuration audits of all systems.

6.2.1 Critical Systems' Configuration

Critical systems contain information that is essential for the on-going conduct of business .

Critical systems should remain in tested configurations (hardware and software) which can be reproduced. Plans to modify any such configuration should contain appropriate backout plans should unforeseen difficulties occur. Any modifications should be disseminated to all affected individuals prior to the installation. Additional resources to create model or test environments may be required.

6.2.2 Software Licenses

Winona County purchases software licenses for installation on all Winona County authorized systems. Installation on systems at non-Winona County facilities (including Winona County staff home systems) is permitted if the software license allows it. Additional uses of Winona County licenses are not allowed.

Software licenses and pertinent information should be stored and maintained in a central location for all software owned by the County.

Note: In many cases a “license” is conveyed only by a sales receipt or paid invoice.

6.2.3 Introduction of External Software

Winona County staff are expressly prohibited from installing any external software on any Winona County information system. This is specified in the Acceptable Use Guidelines as well. Installation of new software should be done only under the authority of the designated system administrator.

External software includes commercial software, shareware, freeware, or Internet-loaded plug-ins and patches.

Note: It is the intent of this guideline to eliminate unlicensed or improperly licensed software on Winona County systems. If such software is discovered on Winona County systems, Winona County, and its staff and users of that system could be subject to legal action by the software vendor.

6.3 Physical Access Control

Critical information system components including phone systems, servers, routers, and wiring closets should be secured behind locked doors with proper HVAC and AC power conditions. An audit of these elements should be completed and maintained annually.

Note: The security mechanisms of these devices can be easily circumvented if physical access is allowed. Networking components should be secured at all times in a restricted area.

6.3.1 Introduction of New Equipment

Winona County staff should not modify, or allow to be modified, the hardware or software configuration of any computer or communications equipment except under the authority of the Information Technology Director.

This guideline is intended to include such actions as:

- Addition or removal of a modem to a computer or terminal.

- Addition or removal of any computer hardware or peripheral (laptop, printer, scanner, disk drive, tape drive, memory).

- Addition or removal of any software or software configurations.

6.3.2 Automatic Logout

Where technically possible, computer systems should detect when a period of inactivity and either log the user out or activate a password protected screen saver.

The length of inactivity, which is acceptable, should be determined for each computer environment.

6.3.3 Environmental Control

The environment in which a computer system operates can have a dramatic effect on the stability of the computer system, and therefore the data, which resides upon it. Critical networking systems like routers and servers must be protected by some power filtering system such as an uninterruptible power supply (UPS). UPS devices with integrated surge protection are strongly recommended.

6.4 Virus Control

All Winona County computers should have installed an up-to-date virus scanning software package. This package should be configured to scan floppies upon insertion, scan the hard drive and boot sector on boot up, and be able to scan a field/directory/drive on disk insertion.

Note: Subscription updates are a vital part of maintaining useful virus protection and must be considered non-optional.

6.4.1 New Software Virus Scanning

All personal computer software should be scanned for viruses with an up-to-date virus scanning software package before being installed on any computer.

6.4.2 Virus Containment

Winona County staff should notify the system administrator immediately if they suspect or confirm that their computer system has been infected with a virus. Only properly trained individuals should attempt to destroy or remove a virus.

6.4.3 Anti-Virus Software on Servers

Winona County servers should be protected by including server-based anti-virus software on every server installation. This software provides for continuous scanning of files it receives from workstations, and has an updateable virus signature file.

6.5 Backup

Periodic backups should be performed on all Winona County servers. The ideal back-up standard is a daily-run full-image backup for every server in daily use. Backup storage should contain enough space for weekly and monthly images.

All system backups should be protected with the same types of measures as used on the on-line system that has been backed-up. Backups should be stored in off-site locations to help minimize the chances that the backup media would be damaged with the computer system.

6.5.1 Testing of Backups

This Guideline recommends that authorized system administrators perform data restorations once per month as spot checks, and that system administrators perform a whole-system restore once per year.

6.5.2 Restoration of Backups

ONLY authorized system administrators or operators should perform data restorations.

6.5.3 Individual Backups

Winona County staff should not store files on their local computer. All files stored on “home” directories will be backed up daily. Files no longer used should be removed from County servers and systems.

6.6 Disaster Recovery

All critical and sensitive systems should have a tested Information Security Disaster Recovery Plan. County Computer Coops are coordinating this activity statewide.

6.7 County-Approved Information Server for Staff, Public Notices and Governmental Information.

6.7.1 Official Publication

Winona County may maintain one or more WWW servers for staff and public access. This server is an official publication of the County, to be used for communications and notices among employees, officials and staff. It is similar in scope and requirements to a newsletter or press release published by the County, and should be reviewed and regarded in this light.

6.8 E-mail

Winona County authorizes and maintains e-mail and servers for staff use. These servers are all “official” publications of the County.

The content of e-mail is stored on Winona County servers, and should be considered to be non-private in nature. System administrators may need to access materials contained in these e-mail accounts. Personal and non-governmental-related account material should not be stored on the Winona County servers.

6.8.1 Staff E-mail Accounts

Use of official E-mail constitutes the creation of a public document and is to be used for communications in fulfillment of the governmental mission of the County.

6.8.1.1 Retention of E-mail Records

E-mail server backups will be retained in the same schedule as established records retention schedules dictate for paper documents and correspondence.

7. Training

Winona County department heads or supervisors will establish and maintain a security awareness-training curriculum that all department staff should review.

Note: Security awareness, password selection and appropriate use should be major focuses of this training.

8. Enforcement

Enforcement of this Security Policy will be taken seriously. These guidelines are put in place for the protection of Winona County information resources as they support the mission of Winona County. Compromise of data could result in embarrassments, negative public relations, and liability issues.

8.1 Disciplinary Action

Disciplinary action for intentional or unintentional violation of these guidelines is covered by the Winona County Personnel Policies.

8.2 Reporting Problems (and Maintenance of Confidentiality)

If a Winona County professional has knowledge of, or suspicion of a compromise or attempted compromise of Winona County information systems, or access controls, that staff member is expected to report that knowledge or suspicion immediately upon becoming aware of the potential security problem to their supervisor or to a system administrator. Such reports will be considered confidential communications akin to "whistleblower" reports, and will not result in retaliation against the reporter.

Note: The purpose of this Guideline is to increase system integrity in Winona County because even seemingly minor or trivial actions or changes to systems can snowball into major breakdowns.

8.3 Automatic Logging and Commitment or Monitor Logs

"Security relevant" activities should be logged, and staff resources allocated for periodic spot-checks of security-relevant data.

Security logs should be reviewed and analyzed on a periodic and timely basis to help ensure that Winona County information systems remain in as secure an operating condition as possible.

9. Records Retention

Each Winona County department will establish and maintain a records retention policy consistent with Minnesota statutes, that all staff members should receive training on and review periodically.