CITY OF UKIAH

IT Policies and Guidelines

CITY OF UKIAH

Table of Contents

Policies

Other documentation

CITY OF UKIAH

Network Connection Policy

1.0 Purpose

This policy is designed to protect the campus network and the ability of members of the City of Ukiah community to use it. The purpose of this policy is to define the standards for connecting computers, servers or other devices to the city's network. The standards are designed to minimize the potential exposure to the City of Ukiah and our community from damages (including financial, loss of work, and loss of data) that could result from computers and servers that are not configured or maintained properly and to ensure that devices on the network are not taking actions that could adversely affect network performance.

City of Ukiah must provide a secure network for our civic, research, instructional and administrative needs and services. An unsecured computer on the network allows denial of service attacks, viruses, Trojans, and other compromises to enter the city’s network, thereby affecting many computers, as well as the network's integrity. Damages from these exploits could include the loss of sensitive and confidential data, interruption of network services and damage to critical City of Ukiah internal systems. Entities that have experienced severe compromises have also experienced damage to their public image. Therefore, individuals who connect computers, servers and other devices to the city’ network must follow specific standards and take specific actions.

2.0 Scope

This policy applies to all members of the City of Ukiah community or visitors who have any device connected to the City of Ukiah network, including, but not limited to, desktop computers, laptops, servers, wireless computers, specialized equipment, cameras, environmental control systems, and telephone system components. The policy also applies to anyone who has systems outside the campus network that access the campus network and resources. The policy applies to city-owned computers (including those purchased with non-IT funds), personally-owned or leased computers that connect to the city network.

3.0 Policy

3.1 Appropriate Connection Methods

You may connect devices to the campus network at appropriate connectivity points including voice/data jacks, through an approved wireless network access point, via a VPN or SSH tunnel, or through remote access mechanisms such as DSL, cable modems, and traditional modems over phone lines.

Modifications or extensions to the network can frequently cause undesired effects, including loss of connectivity. These effects are not always immediate, nor are they always located at the site of modifications. As a result, extending or modifying the city network must be done within the IT Department's published guidelines. Exceptions may be made by the IT Department for approved personnel in departments who can demonstrate competence with managing the aforementioned hardware.

3.2 Network Registration

Users of the network may be required to authenticate when connecting a device to it. Users may also need to install an agent on their computers before they are allowed on the network. The role of such an agent would be to audit the computer for compliance with security standards as defined in section 3.4 below.

The IT Department maintains a database of unique machine identification, network address and owner for the purposes of contacting the owner of a computer when it is necessary. For example, the IT Department would contact the registered owner of a computer when his or her computer has been compromised and is launching a denial of service attack or if a copyright violation notice has been issued for the IP address used by that person.

3.3 Responsibility for Security

Every computer or other device connected to the network, including a desktop computer has an associated owner (e.g. an employee who has a personal computer) or caretaker (e.g. a staff member who has a computer in her office). For the sake of this policy, owners and caretakers are both referred to as owners.

Owners are responsible for ensuring that their machines meet the relevant security standards and for managing the security of the equipment and the services that run on it. Some departments may assign the responsibility for computer security and maintenance to the Departmental Computing Coordinator or the Departmental Systems Administrator. Therefore, it is possible that one owner manages multiple departmental machines plus his or her own personal computer. Every owner should know who is responsible for maintaining his or her machine(s).

3.4 Security Standards

These security standards apply to all devices that connect to the City of Ukiah network through standard campus ports, through wireless services, and through home and off campus connections.

- Owners must ensure that all computers and other devices capable of running anti-virus/anti-malware software have city-licensed anti-virus software (or other appropriate virus protection products) installed and running. Owners of non-IT Department managed devices should update definition files at least once per week.
- Computer owners must install the most recent security patches on the system as soon as practical or as directed by IT Security. Where machines cannot be patched, other actions may need to be taken to secure the machine appropriately.
- Computer owners of computers that contain sensitive city data should apply extra protections. The IT Department will provide consultations on request to computer owners who would like more information on further security measures. For instance, individuals who are maintaining files with Social Security information or other sensitive personal information should take extra care in managing their equipment and securing it appropriately.

3.5 Centrally-Provided Network-Based Services

The IT Department, the central computing organization, is responsible for providing reliable network services for the entire city. As such, individuals or departments may not run any service which disrupts or interferes with centrally-provided services. These services include, but are not limited to, email, DNS, DHCP, and Domain Registration. Exceptions will be made by the IT Department for approved personnel in departments who can demonstrate competence with managing the aforementioned services. Also, individuals or departments may not run any service or server which requests from an individual their IT Department - maintained password.

3.6 Protection of the Network

The IT Department uses multiple methods to protect the city’s network:

- monitoring for external intruders
- scanning hosts on the network for suspicious anomalies
- and blocking harmful traffic.

All network traffic passing in or out of the city's network is monitored by an intrusion detection system for signs of compromises. By connecting a computer or device to the network, you are acknowledging that the network traffic to and from your computer may be scanned.

The IT Department routinely scans the city's network, looking for vulnerabilities. At times, more extensive testing may be necessary to detect and confirm the existence of vulnerabilities. By connecting to the network, you agree to have your computer or device scanned for possible vulnerabilities.

The IT Department reserves the right to take necessary steps to contain security exposures to the city and or improper network traffic. The IT Department will take action to contain devices that exhibit the behaviors indicated below, and allow normal traffic and central services to resume.

- imposing an exceptional load on a campus service;
- exhibiting a pattern of network traffic that disrupts centrally provided services;
- exhibiting a pattern of malicious network traffic associated with scanning or attacking others;
- exhibiting behavior consistent with host compromise;

The IT Department reserves the right to restrict certain types of traffic coming into and across the city's network. The IT Department restricts traffic that is known to cause damage to the network or hosts on it, such as NETBIOS. The IT Department also may control other types of traffic that consume too much network capacity, such as file-sharing and streaming media traffic.

By connecting to the network, you acknowledge that a computer or device that exhibits any of the behaviors listed above is in violation of this policy and will be removed from accessing the network until it once again meets compliancy standards.

Acceptable Use Policy

1.0 Purpose

The computing resources at The City of Ukiah support the administrative, instructional, research, and educational activities of the city and the use of these resources is a privilege that is extended to employees of the City of Ukiah. As a user of these services and facilities, you have access to valuable city resources, to sensitive data, and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legal manner.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, the city will take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the City. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet. These policies and laws are subject to change as state and federal laws develop and change.

This document establishes specific requirements for the use of all computing and network resources at The City of Ukiah.

2.0 Scope

This policy applies to all users of computing resources owned or managed by The City of Ukiah. Individuals covered by the policy include (but are not limited to) employees and guests or agents of the administration, external individuals and organizations accessing network services via the City of Ukiah's computing facilities.

Computing resources include all city owned, licensed, or managed hardware and software, and use of the city network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

These policies apply to technology administered in individual departments, the resources administered by central administrative departments, personally owned computers and devices connected by wire or wireless to the City of Ukiah network, and to off-campus computers that connect remotely to the City's network services.

2.1 Your Rights and Responsibilities

As a member of the City community, the city provides you with the use of work-related tools, including access to certain computer systems, servers, software and databases, to the telephone and voice mail systems, and to the Internet.

You are responsible for knowing the regulations and policies of the City that apply to appropriate use of the City's technologies and resources. You are responsible for exercising good judgment in the use of the City's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.

As a representative of the City of Ukiah municipal government, you are expected to respect the City's good name in your electronic dealings with those outside the City.

3.0 Policy

3.1 Acceptable Use

- You may use only the computers, computer accounts, and computer files for which you have authorization.
- You may not use another individual's account, or attempt to capture or guess other users' passwords. [Computing Password Policy]
- You are individually responsible for appropriate use of all resources assigned to you, including the computer, the network address or port, software and hardware. Therefore, you are accountable to the City for all use of such resources. As an authorized The City of Ukiah user of resources, you may not enable unauthorized users to access the network by using a City computer or a personal computer that is connected to the City network. [Network Connection Policy]
- The City is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources.
- You should make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access. You must configure hardware and software in a way that reasonably prevents unauthorized users from accessing City's network and computing resources.
- You must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications

without appropriate authorization by the system owner or administrator. [Confidentiality and Safeguarding Information Policy]
- You must comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
- You must not develop or use programs that disrupt other computer or network users or that damage software or hardware components of a system.
- Do not download and/or use tools that are normally used to assess security or to attack computer systems or networks (e.g., password "crackers", vulnerability scanners, network sniffers, etc.) unless you have been specifically authorized to do so by the IT Department.

See Acceptable Use Examples to clarify City's interpretation of acceptable use.

3.2 Fair Share of Resources

The IT Department, and other City departments which operate and maintain computers, network systems and servers, expect to maintain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The City network, application servers, mail servers and other central computing resources are shared widely and are limited; therefore, resources must be used with consideration for others who also use them.

The City may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them. Please review the Fair Share of Resources section of the "Acceptable Use Examples" for further clarification.

3.3 Adherence with Federal, State, and Local Laws

As a member of the City of Ukiah community, you are expected to uphold local ordinances and state and federal law. Some City guidelines related to use of technologies derive from that concern, including laws regarding license and copyright, and the protection of intellectual property.

As a user of City's computing and network resources you must:

- Abide by all federal, state, and local laws.
- Abide by all applicable copyright laws and licenses. The City of Ukiah has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements.

- Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement.
- Do not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless you have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution.

Please review the City’s Copyright Infringement Policy, which details the policies and procedures The City of Ukiah follows in responding to notifications of alleged copyright infringements.

3.4 Other Inappropriate Activities

Use City's computing facilities and services for those activities that are consistent with the public service, educational and research mission of the City. Other prohibited activities include:

- Activities that would jeopardize the City's reputation or status.
- Use of City's computing services and facilities for political or personal economic gain.

3.5 Privacy & Personal Rights

- All users of the city's network and computing resources are expected to respect the privacy and personal rights of others.
- Do not access or copy another user's email, data, programs, or other files without permission.
- Be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is not allowed and could lead to City discipline as well as legal action by those who are the recipient of these actions.

While the City does not generally monitor or limit content of information transmitted on the campus network, it reserves the right to access and review such information. It may exercise this right in investigating performance deviations and system problems, determining if an individual is in violation of this policy, or, as may be necessary, to ensure that City is not subject to claims of institutional misconduct. Access to files on City owned equipment will be approved by specific personnel when there is a reason to access those files. Authority to access user files can come from the City Manager in conjunction with the IT Supervisor. External law enforcement agencies and Public Safety may request access. All such requests must be approved by the City Manager. Information obtained in this manner can be admissible in legal proceedings or in a City hearing.

3.51 Important Notice for Employees:

Electronic information systems and network services are made available for use by employees to conduct City business. Subject to applicable laws, the City, through its authorized officers, reserves and retains the right to access and inspect stored information without the consent of the user. Users are advised that electronic data (and communications using the City network for transmission or storage) may be reviewed and/or accessed by authorized City officials for purposes related to City business. The City has the authority to access and inspect the contents of any City equipment, files or email on its systems. If such circumstances arise where files (including email) are not accessible to authorized City officers due to circumstances such as unexpected absence, death, or termination of employment, the City Manager and IT Supervisor will review a request by an authorized City official and, if appropriate, authorize the specific access as necessary.

3.52 Email

- You should not expect email privacy when connected to the City of Ukiah network. City staff may be exposed to email in the course of their work. Staff is expected to disclose or use this information only when necessary to perform their job duties or when necessary to advance the interests of the City. Remember that email is easily redistributed and may be read by people beyond the original recipient list.
- Remember that email is easily redistributed and may be read by people beyond the original recipient list.
- All postscripts should be limited to providing what is commonly known as signature information about the sender (name, title, contact information, address, and statements regarding confidentiality of the communication).

Please see City's Electronic Mail Policy for further details on this service.

3.6 User Compliance

When you use City computing services, and accept any City issued computing accounts, you agree to comply with this and all other computing related policies. You have the responsibility to keep up-to-date on changes in the computing environment, as published, using City electronic and print publication mechanisms, and to adapt to those changes as necessary.

City of Ukiah

Computer Logon Banner

Purpose:

The banner below is displayed prior to the logon of all Windows systems. It is used as a form of acknowledgement and reminder that the user of any the City of Ukiah's Information Systems may be monitored.

WARNING: Use of this System is Restricted and Monitored!

This system is for the use of authorized users only. Individuals using this computer are subject to having all of their activities on this system monitored and recorded by system personnel. Anyone using the system expressly consents to such monitoring. If such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Confidentiality and Safeguarding Electronic Information Policy

1.0 Purpose

This document establishes specific requirements for the proper protection of electronic information resources and to ensure that the City of Ukiah maintains strict confidentiality in compliance with applicable requirements, regulations and laws.

2.0 Scope

This policy pertains to the security and privacy of all electronic non-public information including employee information, constituent information and general city information. Accordingly, electronic documents that include confidential information such as social security numbers, dates of birth, education records, medical information, benefits information, compensation, loans, or financial aid data, and staff evaluations need to be secured during printing, transmission (including by fax), storage and disposal.

3.0 Policy

All employees and users of networked computing devices on city's network have a role in protecting the City of Ukiah's information assets because their machines provide potential gateways to private information stored elsewhere on the network. Therefore, whether or not you deal directly with sensitive or confidential city information, you should take the following steps to reduce risk to the City of Ukiah's information assets.

3.1 General Guidelines

Care and judgment, based on a respect for individual privacy and concern for the City's interests, must be exercised to ensure confidentiality.

- Do not leave electronic documents containing confidential information unattended on computer screens; protect them from the view of passers-by or office visitors.
- Store electronic documents containing confidential information on unencrypted devices that may leave City facilities.
- Immediately retrieve or secure sensitive documents that are printed on copy machines, fax machines and printers.
- Theft of the City of Ukiah electronic computing equipment must be immediately reported to the IT Department or Purchasing; loss or suspected compromise of City of Ukiah sensitive or confidential data must be immediately reported to the IT Department.

First, Educate Yourself

- Read the City of Ukiah's IT Policies, and understand their implications for the information for which you are responsible.
- Immediately advise IT Department of any suspicious activity on your computer or a suspected information system security compromise. The IT Department will determine if follow-up action is required.
- Be mindful of how you are sharing or transmitting sensitive information across the network.

Protecting E-Mail

- Understand that e-mail is not secure; it can be forged, and it does not afford privacy.
- Do not open unexpected e-mail attachments, and do not download documents or software from unknown parties.
- Clear e-mail boxes of old messages on a regular basis.
- Take precautions not to send anything by e-mail that you wouldn't want disclosed to unknown parties. Recipients have been known to distribute information to unauthorized recipients or store it on unsecured machines, and viruses have been known to distribute archived e-mail messages to unintended recipients.

Restrict Access to Information on Your Desktop

- Orient your computer screen away from the view of people passing by.
- Turn off your desktop computer at the end of the workday, unless automatic updates, backup processing, and/or various other maintenance operations are scheduled during off-hours.
- Use password-protected screensavers on your desktop computer.
- Use security devices to lock down computers that are in public or otherwise unsecured spaces.
- Ensure that functions that enable data sharing on an individual workstation are either turned off or set to allow access only to authorized personnel.

Secure Mobile & Cellular Devices

Information stored on laptop computers, personal organizers (e.g., PDAs, Blackberry, Palms), cellular phones, and other similar mobile devices is susceptible to equipment failure, damage, or theft. Information transmitted via wireless connections is not always secure - even networks using encryption are vulnerable to intruders.

- Protect and secure mobile devices from theft at all times.
- Use internal firewalls and strong authentication when transmitting information via wireless technologies.
- Use personal firewalls and VPN on laptops that will access the network from a remote location.
- Back up the data on your mobile devices on a regular basis.
- Change batteries on mobile devices as soon as the "low battery" prompt appears to avoid losing information, configurations, and settings.

Protecting Passwords

- Adhere to the City of Ukiah's Password Policy.
- Employ passwords that are easy for you to remember but impossible for someone else to guess:
  - Passwords should not consist of a word that can be found in a dictionary.
  - Passwords should be at least 8 characters in length and consist of a combination of numeric characters, mixed upper and lower case alpha characters, and at least one special character.
  - Consider using the first letter of each word in a phrase or sentence that you can easily remember. For example, "aLi#1imb" is derived from "Abe Lincoln is #1 in my book."
- Secure your passwords, and restrict access to them. Passwords written on a post-it in a work area, placed under a keyboard, or stored in an unlocked desk drawer are not safe from unauthorized access.
- Never share your passwords or accounts.
- Change your passwords at least every 3 months. The more sensitive the information being protected, the more frequently you should consider changing your passwords.

Protecting the Integrity of Information

- Apply system updates for your desktop systems and department servers' operating systems and their integrated network services (e.g., e-mail and web browsers) in a timely manner.
- Keep local applications updated and patched. (Contact the IT Department for guidance.)
- Encrypt sensitive files. Use IT Security-approved encryption methods only.

- Secure local servers in a locked room and limit the access to the room to system administrators only.
- Ensure that remote access connections are done securely using SSH or VPN.

Back Up Information

- Know the back-up and recovery strategies for the information for which you are responsible.
- Know whether your data is backed up centrally and/or locally.
- Know the frequency with which the back-ups occur.
- Know who is responsible for backing up your information.
- Make sure that the recovery procedures for your information have been tested.
- Know where your back-ups are stored.
- Store back-ups of critical information in an alternate location, preferably in another building across campus or off-site.
- Make sure that private information stored on back-ups in alternate locations is protected from unauthorized access.
- Know how you will recover critical data and resume related business operations in the event of loss of power, disruption of network services, theft of your computing device, or inability to access your office or building.

Assistance

- Contact the IT Department first for assistance with any questions you might have. The IT Department can be reached at (707)463-6229
- Always feel free to contact the IT Supervisor directly if you have questions. Steve can be reached at sbutler@cityofukiah.com or at 463-6209.

3.2 Non-Disclosure and Non-Use

Employees may not disclose to unauthorized persons or use for their own personal benefit or profit of another, any confidential electronic information that they obtain as a result of their employment at city. This obligation continues after an employee's employment with the city ends.

3.3 Access

The City of Ukiah will maintain strict control over access to work locations containing IT equipment, electronic records, computer and network information, other sensitive network items. Employees who are given special access or assigned job responsibilities in connection with the safety, security or confidentiality of such records, materials, equipment, or items of value will be required to use sound judgment and discretion in carrying out their duties and will be held accountable for any wrongdoing or acts of indiscretion. Furthermore, electronic information may not be divulged, copied, released, sold, loaned, reviewed, altered or destroyed except as properly authorized within the scope of applicable federal, state or local laws.

3.4 Policy Summary

Access to proprietary electronic information will be limited to those who need the information in order to fulfill his or her professional responsibilities. At the beginning of their employment with the City of Ukiah, employees agree that they will not disclose proprietary City electronic information to any other person or entity without prior authorization. A copy of the Rules of Behavior Agreement must be signed and kept on file in the employee's personnel record before gaining access to the City's .

At the conclusion of employment with the City of Ukiah, all employees are required to return all electronic City documents and records, especially those containing proprietary information. Employees are also required to maintain the confidentiality of City information even if they leave employment. Questions regarding the City's proprietary information should be directed to the employee's supervisor or Human Resources Department.

CITY OF UKIAH

Computing Passwords Policy

1.0 Purpose

This policy describes the City of Ukiah's requirements for acceptable password selection and maintenance. It provides guidance on creating and using passwords in ways that maximize security of the password and minimize misuse or theft of the password.

Passwords are the most frequently utilized form of authentication for accessing a computing resource. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity of malicious hackers and spammers, they are very often also the weakest link in securing data. Passwords must therefore follow the policy guidelines listed below.

2.0 Scope

This policy applies to anyone accessing systems that hold or transmit City of Ukiah data. Systems include, but are not limited to: personal computers, laptops, city-issued cell phones, and small factor computing devices (e.g., PDAs, USB memory keys, electronic organizers), as well as city electronic services, systems and servers. This policy covers departmental resources as well as resources managed centrally.

3.0 Policy

All passwords (e.g., email, web, desktop computer, etc.) should be strong passwords and should follow the guidelines below. In general, a password's strength will increase with length, complexity and frequency of changes.

Greater risks require a heightened level of protection. Stronger passwords augmented with alternate security measures such as multi-factor authentication, should be used in such situations. High risk systems include but are not limited to: systems that provide access to critical or sensitive information, controlled access to shared data, a system or application with weaker security, and administrator accounts that maintain the access of other accounts or provide access to a security infrastructure.

Central and departmental managers and/or system administrators are expected to set a good example through a consistent practice of sound security procedures.

1. All passwords must meet the following guidelines, except where technically infeasible:
    - be at least eight alphanumeric characters long.
    - The password must meet the following requirements:
        1. contain an upper case character (e.g., A-Z).
        2. contain a lower case characters (e.g., a-z).
        3. contain digits or punctuation characters (e.g., !@#$%^&()_~-=`{}".') **OR** contain a number (e.g., 123)
    - not be a word in any dictionary, language, slang, dialect, jargon, etc.
    - not be solely based on easily guessed personal information, names of family members, pets, etc.
2. To help prevent identity theft, personal or fiscally useful information such as Social Security or credit card numbers must *never* be used as a user ID or a password.
3. All passwords are to be treated as sensitive, confidential information and should therefore never be written down or stored on-line unless adequately secured. ***NOTE:*** *Do not use the password storage feature offered on Windows or other operating systems. This feature creates a password file that is vulnerable to hackers.*
4. Passwords should not be inserted into email messages or other forms of electronic communication without the consent of the IT Department.
5. Passwords that could be used to access sensitive information must be encrypted in transit.
6. The same password should not be used for access needs external to the City of Ukiah systems (e.g., online banking, benefits, etc.).
7. It is recommended that passwords be changed at least every three months.
8. Passwords should not be shared with anyone, including administrative assistants or IT administrators. Necessary exceptions may be allowed with the written consent of the IT Department and must have a primary responsible contact person. Shared passwords used to protect network devices require a designated individual to be responsible for the maintenance of those passwords, and that person will ensure that only appropriately authorized employees have access to the passwords.
9. If a password is suspected to have been compromised, it should be changed immediately and the incident reported to the IT Department.
10. Password cracking or guessing may be performed on a periodic or random basis by the IT Department or its delegates. If a password is

guessed or cracked during one of these scans, the password owner will be required to change it immediately.

NOTE: Consult the Password FAQ for suggestions on forming strong passwords and the use of passwords at the City of Ukiah.

3.1 Desktop Administrator Passwords

In addition to the general password guidelines listed above in Section 3.0, the following apply to desktop administrator passwords, except where technically and/or administratively infeasible:

1. These passwords must be changed at least every six months.
2. Where technically and administratively feasible, attempts to guess a password should be automatically limited to ten incorrect guesses. Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes.
3. Failed attempts should be logged, unless such action results in the display of a failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities or compromises should be immediately reported to the IT Department.

3.2 Server Administrator Passwords

In addition to the general password guidelines listed above in Section 3.0, the following apply to server administrator passwords, except where technically and/or administratively infeasible:

1. Passwords for servers must be changed as personnel changes occur.
2. If an account or password is suspected to have been compromised, the incident must be reported to the IT Department and potentially affected passwords must be changed immediately.
3. Attempts to guess a password should be limited to ten incorrect guesses. Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes.
4. Uniform responses should be provided for failed attempts, producing simple error messages such as "Access denied". A standard response minimizes clues that could result from hacker attacks.
5. Failed attempts should be logged, unless such action results in the display of the failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities such as suspected attacks should be reported to the IT Department.

NOTE: Log files should **never** contain password information.

Electronic Mail Policy

1.0 Purpose

The purpose of this policy is to ensure that the City of Ukiah's electronic mail (e-mail) services remain available to and reliable for the organization, and are used for purposes appropriate to the City's mission.

2.0 Scope

This policy applies to all employees and authorized users of the City of Ukiah who are entitled to email services.

3.0 Policy

3.1 Use of the City of Ukiah Email Addresses and Accounts

While a person is a user of the city’s systems, email is a means of official communication to that person. As such, official city communication mechanisms (including but not limited to: urgent bulk email, course email, and Morning Mail) should be read on a regular basis since they may affect day-to-day activities and responsibilities.

IT provides central electronic mailbox services. A person may not have his or her email delivered to a non IT-managed mailbox or forwarded to another mail repository. Because of the confidential nature of some content transmitted via email by staff, staff is limited to using central services or forwarding to a departmental server within the City of Ukiah address space.

3.2 Email restrictions and storage limits

To manage the storage requirements of our email system the following restrictions and limits have been put into place.

Email size: Emails in excess of 10 MBs (megabytes) will not be accepted by our email system. If you have a requirement to distribute files that exceed this limit please utilize our shared files drives or contact the IT Helpdesk for assistance.

Mailbox storage limits: When your account is created you are granted 200 MBs of storage for your mail. This would be for storage of your email, calendar, tasks and contacts. The following rules are enacted if you exceed your limits:

>200 MBs: You will receive a warning email explaining you’ve exceeded your limit. At this point there is no effect to your account.

>250 MBs: You will receive an email explaining you have exceeded your limit, additionally you will no longer be able to send email. You will still receive email at this point.

>350 MBs: You will receive another email explaining you’ve exceeded this limit AND that you will no longer be able to send OR receive email. Additonally anyone attempting to send you email will get a notice that your mailbox is full and not accepting any more messages.

Dropping the size of your mailbox below the limits will immediately restore your ability to send and receive email.

3.3 Protection of Electronic Communications Services

Inbound Email

IT systems scan inbound email for content that may be characterized as spam. Where spam characteristics are found, the message may be tagged (through an update to the headers) or quarantined. IT also routinely scans all email for viruses and trojans. The scanning for viruses and trojans may also lead to a modification of the headers of the email, or further consequences, as explained below.

Because of the potentially harmful nature of the content of many messages or attachments, IT currently:

- Does not deliver messages containing attachments that have been identified as worms by our current anti-virus vendor;
- Deletes attachments that are identified as containing viruses by our current anti-virus vendor;
- Blocks messages from external mailers that do not provide the proper identification per DNS. (Some spammers make use of improperly configured SMTP servers in an attempt to mask their true identity.)

IT reserves the right to block other incoming email that exhibits characteristics of spam, viruses, trojans, or anything else that could threaten the network infrastructure or services.

Outbound Email

- All outbound email must be routed through central mail relay services, or through an authorized departmental mail relay service.
- Messages up to 10 MB in size (including attachments) may be sent through city's mail services.
- Outbound email will be scanned for viruses.

3.4 Misuse of Email

The City of Ukiah email services may not be used to send unsolicited bulk or commercial email. They may not be used to send messages (such as large volumes of email messages or extremely large individual email messages) with the intent of disrupting a server or an individual's account on a server.

To protect the availability of the email service at the city, users should refrain from sending chain letters, holiday cards or similar items to more than a few people. Unauthorized messages sent to large groups can impact central services in an adverse manner. If a user has questions about whether or not to send a message to a large distribution, that individual should check with a supervisor or contact the City of Ukiah IT Department.

Forging, altering, or removing of electronic mail headers is also prohibited.

Violation of this or any other City of Ukiah policy may result in disciplinary action, up to and including suspension or termination.

3.5 Departmental Email Boxes

Departments that provide services in response to email requests should create departmental email boxes. These will provide continuity as individual employees move into and out of various departmental roles, assuring that important email requests for services will be appropriately directed to the person who can handle the request. Privileges to access these shared email boxes will be managed by the mailbox "owner", a department head or delegate.

Copyright Infringement Policy

Copyright Law, the Illegal Use of File Sharing Programs, City of Ukiah Policies and Procedures for Handling Violations

This document is intended to explain the policies and procedures the City of Ukiah follows in responding to notifications of alleged copyright infringements on the city's network.

What is copyright?

Copyright is legal protection of intellectual property, in whatever medium, that is provided for by the laws of the United States to the owners of copyright. Types of works that are covered by copyright law include, but are not limited, to literary, dramatic, musical, artistic, pictorial, graphic, film and multi-media works. Many people understand that printed works such as books and magazine articles are covered by copyright laws but they are not aware that the protection extends into software, digital works, and unpublished works and it covers all forms of a work, including its digital transmission and subsequent use.

What is the current law concerning digital copyright?

The Digital Millennium Copyright Act (DMCA), signed into law in 1998, recognizes that digital transmission of works adds complexity to the Copyright Law. The DMCA provides non-profit institutions with some protections if individual members of the community violate the law. However, for the City of Ukiah to maintain this protection we must expeditiously take down or otherwise block access to infringing material, whenever it is brought to our attention and whether or not the individual who is infringing has received notice.

Individuals can be subject to the imposition of substantial damages for copyright infringement incidents relating to the use of City network services. In a civil action, the individual infringer may be liable for either actual damages or statutory damages of up to $30,000 (which may be increased to up to $150,000 if the court finds the infringement was willful). In addition, individual infringers may be subject to criminal prosecution. Criminal penalties include up to ten years imprisonment depending on the nature of the violation.

Why is it an important issue right now?

Copyright is an issue of particular seriousness because technology makes it easy to copy and transmit protected works over our networks. The City of Ukiah does not condone the illegal or inappropriate use of material that is subject to copyright protection and covered by state and federal laws.

What kinds of activities violate the federal law?

Following are some examples of copyright infringement that may be found in a networked setting:

- Downloading and sharing MP3 files of music, videos, and games without permission of the copyright owner
- Using corporate logos without permission
- Using music that is downloaded and artwork that is scanned from a book, all without attribution or permission of the copyright owners
- Scanning a photograph that has been published and using it without permission or attribution
- Downloading licensed software from non-authorized sites without the permission of the copyright or license holder
- Making a movie file or a large segment of a movie available without permission of the copyright owner

Specifically, is sharing and downloading MP3 files and videos illegal?

It is true that some copyright holders give official permission to download MP3 files and you might be able to find a limited number of videos that are not copyright protected. It is also true that some MP3 files are copyright free and some MP3 files can be legally obtained through subscription services. However, most MP3 and video files that are shared do not fall into any of these categories.

US Copyright Law allows you to create MP3s only for the songs to which you already have rights; that usually means you purchased the CD or tape. And US Copyright Law allows you to make a copy of a purchased file only for your personal use. Personal use does not mean that you can give a copy to other people, or sell a copy of it.

How do you get caught violating copyright law?

Copyright holders represented by organizations such as the Recording Industry Association of America, the Business Software Association, and the Motion Picture Association of America are applying serious efforts to stop the infringing downloads of copyrighted music, movies, and software. The companies or their agents locate possible copyright infringements by using automated systems, or "bots" that search the networks looking to see if any of the common music, movie or software sharing programs are active on a port (e.g. KaZaA, Gnutella). The bot then asks the sharing program if it has a music title by a particular artist. If the sharing program answers positively, the bot reports the particular IP address and title to an authority, who then sends out the violation notices to the owners of the IP address.

The City of Ukiah's network has a range of IP addresses and all computers connected to the city network have an IP address. When we get a violation notice, the IT Department locates the IP address and whenever possible, the user of that address. At that point, the City of Ukiah is required to act on the notification.

If the IP address leads to my computer, what happens next?

These notices come to the IT Supervisor from organizations that represent the artists and copyright holders. When we receive such a notice, staff in IT looks up the network IP address and stop network services to the port that is connected to the computer where the infringing material resides. At this point, the computer cannot use any city resources or Internet resources. Once the identity of the individual is known, they are notified that they must remove the infringing material from their computer and inform the IT Department of its removal before network access will be reinstated.

First-time Notifications: If this is the first notification that the City of Ukiah has received on an individual, IT will verify that the infringing material has been removed from the computer. Once this is done, the network connection will be reinstated and the computer can return to the network. A report about the violation of copyright will be sent by the IT Department to the Human Resources Department for inclusion in your personnel file.

Second Notification Process: The City of Ukiah is obligated to exercise greater responsibility to address instances of repeated infringing activity by individuals. There are potentially serious implications for both the individual and the organization if the city receives more than two notices of infringement against an individual within a three-year period. For this reason, in an instance of a second notification of an individual's infringing activities the City Manager and City Attorney are also notified of the infringement and a meeting with the relevant supervisors will be held to determine the action(s) to be taken.

Action Taken in Response to Subpoenas: Upon receipt of a valid subpoena, the City of Ukiah is obligated to turn over any electronic information regarding specific instances of infringing material that has been allegedly transmitted over its networks.

How do you report a copyright infringement?

You can report copyright infringements on the City of Ukiah sites or direct other copyright questions to the IT Helpdesk. You can contact the IT Helpdesk at:

Information Technology Helpdesk
Email: itdept@cityofukiah.com

Phone: (707) 463-6229 | Fax: (707) 463-6740
City of Ukiah | Information Technology Department | 411 West Clay Street |
Ukiah, CA 95482

Frequently Asked Questions about Passwords

The following questions and answers will help you understand more about what passwords are used for at the City of Ukiah, the importance of password security, and how to choose a good password. You should also familiarize yourself with the city's password requirements detailed in its Computing Passwords Policy.

Obtaining and Using Passwords at the City of Ukiah

- What other accounts and passwords does the IT Department manage?
- How can I change my password?
- What do I do if I forget my password?

Choosing a Good Password

- What are the basic password guidelines at the City of Ukiah?
- Complex passwords are harder to remember, especially those with numbers and special characters. Won't any password be sufficient?
- What are some strategies for choosing a good password?

Securing Your Password

- Why should I care about password security?
- How does someone steal a password?
- Why do people steal passwords?
- How often should I change my password?

Obtaining and Using Passwords at the City of Ukiah

What accounts and passwords does the IT Department manage?

Administrative systems such as GFS (Government Financial System) and Utility Billing have accounts that are managed by the IT Department.

How can I change my password?

You can change your password yourself but you will need to login first using your current password to do so. After logging in press the keys <Ctrl><Alt><Del> simultaneously, then click the Change Password button. You will need to enter the new password twice following the Computing Password Policy.

What do I do if I forget my password?

If you forget your password, you can get it reset during the business day. Contact the IT Department at x6229 for assistance.

Choosing a Good Password

What are the basic password guidelines at the City of Ukiah?

The City of Ukiah's Computing Passwords Policy provides guidance on creating and using passwords in ways that maximize security of the password and minimize misuse or theft of the password. A complete list of requirements for a good, strong password can be found there. The bottom line is:

- Never choose an easy-to-guess password. Personal information which can be easily obtained by crackers should never be used in passwords. Examples of extremely bad passwords are words such as your significant other's name, your children's names, your birthday, your dog or cat's name, your favorite NFL team, etc.
- Do not choose passwords such as "rainbow1" (a simple lowercase word followed by a digit) just to satisfy the restrictions used by the IT Department. These passwords are also very easy to crack.
- Choose a difficult password, but not one so difficult that you cannot remember it. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W_r~" or some other variation. **NOTE: Do not use either of these examples as passwords!**
- Do not write down your password (unless you adequately secure it).

Regardless of the password you choose, it is important to remember one critical rule: NEVER share it.

Complex passwords are harder to remember, especially those with numbers and special characters. Won't any password be sufficient?

The use of complex combinations of characters is required to guard against the increasingly sophisticated automatic password-cracking mechanisms that now proliferate. The more complex the combination of characters used, the greater the chance that password crackers will fail. Brown's networks are continuously scanned, internally and externally, from all parts of the globe, and if there is a weak password to be had, it will be found and used to gain entry. Computers may be protected through the use of anti-virus software, personal firewalls, secure configurations, etc., but should the computer have a weak password, it can be cracked almost instantaneously and its contents and connection compromised.

What are some strategies for choosing a good password?

Here are some suggestions from a password FAQ at Duke University:

- **Use lines from a childhood verse**
  Verse Line: Yankee Doodle went to town
  Password: YDwto#town
- **Pick letters from a phrase that's meaningful to you**
  Pass Phrase: Do you know the way to San Jose?
  Password: D!Y!KtwTSJ?
- **City Expression interspersed with street address**
  Chicago is my kind of town
  Password: C1i2mY1K5o6t
- **Foods disliked during childhood**
  Food: rice and raisin pudding
  Password: ric&rAiPudng

Note: Obviously, you shouldn't use any of the passwords used as examples in this document. Treat these examples as guidelines only.

Securing Your Password

Why should I care about password security?

The information that your account has access to may be of a confidential nature and/or important to the city and it is your responsibility to keep it secured. If someone were to get into your account, they may see information such as: social security numbers and names, credit card numbers, disciplinary information about employees, etc. Should any of this information be read by someone who is not authorized to see it, the City of Ukiah, your department, or even individual users may have legal liability. Even your own email communications could be read and shared on the Internet.

How does someone steal a password?

There are dozens of password cracking programs available freely on the Internet. These programs can be used to repeatedly try to access your account, and are set up to try dictionary words, variations on them, and more. That's why we have the requirements and guidelines that we do.

Why do people steal passwords?

People steal passwords for a variety of reasons. Sometimes it is just a game. Other times, they want to use your account, or even your computer, for their own reasons, whether for monetary gain, political statements, or some other agenda.

How often should I change my password?

You will be required to change your password every 3 months. You may even want to do it more frequently. Changing it very frequently can be worse than not changing it at all, however, since you may be tempted to write it down since you are more likely to forget a password you use for a short time.

Information Systems Rules of Behavior Agreement Form

As a user of the City of Ukiah Information Systems, I acknowledge my responsibility to conform to the following requirements and conditions as directed in part by the Network Connection, Acceptable Use, Confidentiality, Password, Electronic Mail, and Copyright Infringement Policies. These conditions apply to all City Employees (Full and Part-time), contractors and anyone else using the City of Ukiah Information Systems.

1. I understand that failure to agree to this acknowledgement will result in denial of access to the City of Ukiah Information Systems and/or facilities.

2. I acknowledge my responsibility to use the network only for official government business except for such personal use involving negligible cost to the Government and no interference with official business as may be permissible under applicable City of Ukiah Information Systems policies.

3. I understand the City of Ukiah Information Systems networks operate at different classification levels. I will not access networks unless I have the proper clearances necessary for access to the networks, and will not introduce or process data that the network is not specifically approved to handle.

4. I understand the need to protect my password and/or account. I will NOT share my password and/or account. I understand that the Information Technology group will never request my password. I will change my password once every 90 days or as requested for security reasons.

5. I understand I am responsible for all actions taken under my account. I will not attempt to "hack" the networks or any connected Information System, or attempt to gain access to data for which I am not specifically authorized.

6. I understand my responsibility to appropriately protect all output generated under my account, including printed output, magnetic tapes, floppy disks, CD-ROMs, DVDs, flash memory devices and downloaded hard disk files.

7. I understand my responsibility to report any/all Information System or network incidents of improper use to the Information Technology Supervisor or Human Resources Department.

8. I will NOT install/remove/modify any hardware or software unless I have received proper Information Technology Department authorization to do so.

9. I acknowledge my responsibility not to introduce any hardware or software not approved by the Information Technology Department.

10. I acknowledge my responsibility to have all official electronic media virus-scanned by the Information Technology Department before introducing it into the Information Systems or networks, when applicable.

11. I certify I will not load additional software and updates onto government and contractor owned **P**ortable **E**lectronic **D**evices (PEDs) which are approved to process or connect to the City of Ukiah Information Systems unless authorized by and coordinated with the Information Technology Department.

12. I will not connect any PEDs or any peripherals for a PED to any government system (classified or unclassified) while in a City of Ukiah Information Systems controlled facility unless appropriately authorized. This includes connection via MODEM and data ports.

13. I will not connect laptops used to process classified information to the Internet or other unclassified systems unless I have received authorization from the City of Ukiah Information Technology Department. I agree to abide by all instructions provided by the City of Ukiah Information Technology Department and to NOT disable/delete/modify the security measures in place on the system.

14. If the PED is suspected of containing unauthorized classified data and cannot be sanitized, I understand the PED will be permanently retained by the City of Ukiah. This also applies to devices that have been connected to or synchronized with this device.

15. I understand and agree that I am bound by and will not knowingly violate the U.S. Constitution, Federal and State laws, Ordinances of the City of Ukiah or Rules of Behavior. I further understand that I cannot be ordered by any authority to violate the U.S. Constitution or Federal and State laws. I bear sole responsibility and liability for any such violation unless I qualify for an immunity from such liability under applicable law.

16. I further acknowledge my responsibility to conform to the requirements of the Rules of Behavior when using City of Ukiah Information Systems. I also acknowledge that failure to comply with the rules of Behavior may constitute a security violation resulting in denial of access to the City of Ukiah Information Systems, networks, or facilities, and that such violations will be reported to appropriate authorities for further actions as deemed appropriate to include disciplinary, civil, or criminal penalties.

17. I agree I have no expectation of privacy in any equipment or media I use or bring into, or remove from, City of Ukiah Government owned or leased facilities. I consent to inspections by authorized City of Ukiah security personnel, at any time at such City of Ukiah facilities, and agree to make any equipment available for audit and review by authorized City of Ukiah security personnel upon request.

18. I further consent that my use of City of Ukiah or non City of Ukiah owned information systems within City of Ukiah facilities may be subject to system monitoring for law enforcement or other purposes.

19. I agree to all Rules of Behavior for City of Ukiah Information Systems as they may be updated from time to time.

____

Print Employee Name

____________________________________ ________________

City of Ukiah Employee (Signature) Date