County of Humboldt
Information Systems Policy

Section I Overview:

1.1 PURPOSE:

The County of Humboldt has made a large investment in information technology. There is a larger investment of staff effort in data creation, classification, storage, and accessibility.

The purpose of this Information Systems Policy is to guide county departments, agencies, and staff in the installation, operation, and management of County information systems. This Information Systems Policy recognizes interdependent information and Information Technology (IT) infrastructure, and therefore all departments share mutual responsibility for information security.

This Information Systems Policy is intended to ensure departmental and countywide technology investments are appropriately secured and provide Humboldt County users with clear guidelines for the use of information systems.

1.2 SCOPE:

The County of Humboldt's Information Systems Policy is a collection of policy statements regarding the management and use of information systems owned and/or utilized by the County and its staff. The policies address information systems used to process county data. The County of Humboldt reserves the right to change the policies at any time.

1.3 CONTENTS:

This Information Systems Policy is comprised of four (4) sections, each dealing with a specific area. The sections of this Information Systems Policy are:

- Overview
- Computer Systems and Network Security
- Use of Technology Equipment
- Definition of Terms

1.4 RESPONSIBILITIES:

1.4.1 County Administrative Office:

The County Administrative Office is responsible for overall IT integration and alignment with County of Humboldt business processes to include providing guidance and direction, prioritizing investment, allocating resources, and resolving conflicts. Accordingly, the County Administrative Office will verify that adequate support for IT operations and security requirements is planned, resourced, documented, and can be executed promptly. The County Administrative Office will ensure that contracts and other agreements include specific requirements as necessary for IT and that County of Humboldt business plans adequately address, resource, and plan IT requirements.

1.4.2 Information Technology Division:

The Information Technology Division is responsible for all Enterprise Level platforms and conducting investigations into any alleged computer or network security compromises, incidents, or problems. All security compromises or potential security compromises must be immediately reported to the Information Technology Division. Accordingly, the Information Technology Division, in conjunction with Departmental Managers, will perform information systems risk assessments, prepare information systems security action plans, evaluate information security products, and perform other activities necessary to assure a secure information systems environment.

1.4.3 Information Security Officer:

The Information Security Officer is responsible for planning, organizing, and directing the countywide Information Security Program, including IT security awareness, IT risk assessment, IT business impact analysis, IT systems recovery, and IT business continuity. The Information Security Analyst, serving in the capacity as Information Security Officer role, is responsible for the day-to-day management of the County IT Security Team and countywide information security function.

1.4.4 System Administrators:

System Administrators are responsible for acting as information systems security coordinators. These individuals are responsible for establishing appropriate user privileges, monitoring access control logs, and performing similar security actions for the systems they administer. They are also responsible for reporting all suspicious computer and network-security-related activities to the Information Technology Division. System Administrators also serve as local information security liaisons, implementing the requirements of this and other information systems security policies, standards, guidelines, and procedures. Information Technology staff performs this role for many departments. If information systems security is not handled by Information Technology, another department, or group, each County of Humboldt department must designate a liaison to consult with Information Technology Division.

1.4.5 Departmental Managers:

Departmental Managers are responsible for ensuring that this Information Systems Policy is adhered to in their area. Besides funds and staff time needed to meet the requirements of these policies, Departmental Managers are also responsible for making sure that all users are aware of County of Humboldt policies related to computer systems, networks, personal computers, electronic mail, video conferencing, and the Internet.

1.4.6 Information Security Working Group:

The Information Security Working Group (ISWG) is Comprised of departmental representatives and the Information Security Officer. The ISWG will review and suggest updates to the Information Security Program and associated policies, as necessary. Members of the ISWG are security champions for their respective departments. Departmental representatives will work with Departmental Managers, so all data and automated processes have designated owners. The ISWG participates in the development of information security policies and procedures.

1.4.7 Users:

Users are responsible for complying with this and all other County of Humboldt policies defining computer systems, networks, personal computers, electronic mail, and Internet security measures.

1.5 TRAINING:

Departmental Managers must provide an orientation to new users and annual training for all users by reviewing this Information Systems Policy. The purpose of the training will be to ensure that all users affected by this Information Systems Policy are made aware of and adhere to the conditions. Also, Departmental Managers must provide access to IT security trainings like Knowbe4 and ensure staff meet all IT security training requirements.

1.6 ACCEPTABLE USE FORM:

All users of information system resources will be required to sign the County of Humboldt Information Systems Acceptable Use Policy form. The signed form will be kept on file in the department where the employee works. The Departmental Manager will ensure that the employee has access to the Information Systems Policy document and has reviewed it before signing the form. It is further recommended that on an annual basis the Information Systems Policy must be reviewed with each employee.

1.7 EXCEPTIONS:

The County of Humboldt acknowledges that under rare circumstances, certain departments will need to employ systems that are not compliant with this Information Systems Policy. All such instances must be approved in writing and in advance by the county Information Security Officer and the Information Technology Division Director until full compliance can be achieved, subject to review by the ISWG as outlined in Section 1.4 of this Information Systems Policy.

1.8 VIOLATIONS:

Users who violate this Information Systems Policy will be subject to disciplinary action up to and including termination from employment or termination of contracts, as appropriate.

1.9 POLICY DEVELOPMENT AND REQUEST FOR CHANGES:

This Information Systems Policy has been approved by the County Administrative Office, Office of Human Resources and Risk Management, and the Information Technology Division. Requests for changes, additions, or other amendments to this document should be sent to the Information Security Officer.

1.10 CONTACT:

For additional information regarding this Information Systems Policy, contact the Information Technology Division.

Section II Computer Systems and Network Security:

2.1 PURPOSE:

The purpose of this Information Systems Policy is to establish management direction, procedures, and requirements to ensure the appropriate protection of information handled by multi-user computer systems and networks.

2.2 SCOPE:

This Information Systems Policy applies to all County of Humboldt employees and any and all contractors, consultants, vendors, and other third parties doing business with the County of Humboldt, including, without limitation, individuals affiliated with third parties who access County of Humboldt computer networks. Throughout this Information Systems Policy, the word "user" will be used to collectively refer to all such individuals. This Information Systems Policy also applies to all data, computers, computer systems, electronic storage media, video conferencing, and/or computer networks owned, and/or administered, by the County of Humboldt.

2.3 GENERAL POLICY:

All information traveling over the County of Humboldt computer networks that has not been specifically identified as the property of other parties will be treated as though it is a County of Humboldt asset. It is the policy of the County of Humboldt to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of such information. Also, it is the policy of the County of Humboldt to protect information belonging to third parties--that has been entrusted to the County of Humboldt in confidence--in the same manner as County of Humboldt information as well as following applicable contracts.

2.4 SYSTEM ACCESS CONTROL:

2.3.1 User Passwords:

Passwords should not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover them.

Passwords should not be written down and left in a place where unauthorized persons might discover them. Aside from initial password assignment and password reset situations, if there is reason to believe that a password has been disclosed to someone other than the authorized user, the password must be immediately changed.

Regardless of the circumstances, passwords should never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the disclosed password. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other mechanisms. This Information Systems Policy does not prevent the use of default passwords for new user-ID assignment or password reset situations which are then immediately changed when the user next logs-onto the involved system.

All passwords should be immediately changed if they are suspected of being disclosed or known to have been disclosed to anyone besides the authorized user.

2.3.2 Password System Set-Up:

All computers permanently, intermittently, or temporarily connected to County of Humboldt networks must have password access controls. Multi-user systems must employ user-IDs and passwords unique to each user, as well as user privilege restriction mechanisms.

Computer and communication system access control must be achieved via passwords that are unique to each user. Access control to files, applications, databases, computers, networks, and other system resources via shared passwords, also referred to as "group passwords," is prohibited, except as explicitly authorized by the Information Security Officer.

Wherever systems software permits, the display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them.

Where possible, all vendor-supplied default passwords must be changed before any computer or communications system is used for County of Humboldt business. This Information Systems Policy applies to passwords associated with end-user user-IDs, as well as passwords associated with System Administrators and other privileged user-IDs.

To prevent password guessing attacks, where systems software permits, the number of consecutive attempts to enter an incorrect password should be strictly limited. After five (5) unsuccessful attempts to enter a password, the involved user-ID should be either suspended until reset by a System Administrator or temporarily disabled for no less than three (3) minutes. If Virtual Private Network (VPN) or other external network connections are involved, the session must be disconnected.

Whenever system security has been compromised or suspected to have been compromised, the involved user should immediately discontinue operations and notify the Information Security Officer.

2.3.3 Log-In/Log-Off Process:

All users must be positively identified before being able to use any IT system resources. Identification for internal County of Humboldt networks involves both a user-ID and password or other authentication tokens, which are unique to an individual user.

Identification for users originating external real-time connections to County of Humboldt systems or networks via public networks, such as the Internet, or any other external communications system must also involve extended user authentication techniques.

Where systems software permits, every log-in banner on multi-user computers should include a special notice. This notice must state that the system is to be used only by authorized users, and by continuing to use the system, the user represents that he/she is an authorized user.

If required by the Departmental Manager, the system should automatically blank the screen and suspend the session when there has been no activity on a computer for a certain time. Re-establishment of the session should take place only after the user has provided a valid password. The recommended time is fifteen (15) minutes. An exception to this process will be made in those cases where the immediate area surrounding a system is physically secured via cipher locks, secured-room badge readers, or similar technology.

2.3.4 System Privileges:

2.4.4.1 Limiting System Access:

The computer and communications system privileges of all users, systems, and independently operating programs, such as “agents,” must be restricted based on the need-to-know. This means that privileges must not be extended unless a legitimate business need for such privileges exists.

County of Humboldt computer and communications systems must restrict access to the computers that users can reach over County of Humboldt networks. These restrictions can be implemented via host and network-based firewalls, endpoint protection, and intrusion prevention systems.

2.4.4.2 Process for Granting System Privileges:

Requests for new user-IDs and changed privileges should be in writing and approved by the user’s Departmental Manager or supervisor before a System Administrator fulfills these requests. To help establish accountability for events on the related systems, documents (perhaps in electronic form) reflecting these requests shall be retained for at least one (1) year in either paper or digital formats.

Individuals who are not County of Humboldt employees must not be granted a user-ID or otherwise be given privileges to use County of Humboldt computers or communications systems without the advance written approval of the Departmental Manager.

Privileges granted to users who are not County of Humboldt employees must be granted for periods of ninety (90) days or less. Users who are not County of Humboldt employees must have their privileges reauthorized by the sponsoring Departmental Manager every ninety (90) days, as needed.

Special system privileges--such as the default ability to write to the files of any other users--must be restricted to those directly responsible for systems administration and/or systems security. An exception to this process can be made only if a department head has approved the exception in writing.

Third-party vendors must NOT be given VPN access to the County of Humboldt computers and/or networks unless the involved System Administrator determines that they have a legitimate need. These privileges must be enabled only for the time required to accomplish the approved tasks, such as remote maintenance. If a perpetual or long-term connection is required, then the connection must be established by approved extended user authentication methods and approved by the Information Security Officer.

All users wishing to use County of Humboldt internal networks or endpoints that are connected to County of Humboldt internal networks, must sign the Humboldt County Information Systems Acceptable Use Policy form before being issued a user-ID.

A signature on the Humboldt County Information Systems Acceptable Use Policy form indicates the user understands and agrees to abide by County of Humboldt policies and procedures related to computers and networks, including, without limitation, the instructions contained in this document.

2.4.4.3 Process for Revoking System Access:

If a computer or communication system access control subsystem is not functioning properly, it must default to denial of privileges to users.

If access control subsystems are malfunctioning, the systems they support must remain unavailable until the problem has been rectified.

Users must not test or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the Information Security Officer. Incidents involving unapproved system compromise or attempted compromises may be unlawful and will be considered serious violations of this Information Systems Policy. Public requests that County of Humboldt security mechanisms be compromised must NOT be satisfied unless:

- The Information Technology Division approves in advance, or
- County of Humboldt is compelled to comply by law. Likewise, short-cuts bypassing systems security measures, as well as pranks and practical jokes involving the compromise of systems security measures are prohibited.

The Departmental Manager must promptly report all significant changes in work duties or employment status to the System Administrators responsible for user-IDs associated with the involved persons.

2.3.5 ESTABLISHMENT OF ACCESS PATHS:

Changes to County of Humboldt internal networks include loading new software, changing network addresses, reconfiguring switches, adding VPNs, and the like. Except for emergencies, all changes to County of Humboldt computer networks must be coordinated with the Information Technology Division. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems. This process applies not only to "users" as defined in the Scope section of this Information Systems Policy but also to vendor personnel.

Users must NOT establish unapproved network or system connections to existing local area networks, or other endpoints for communicating information without the specific approval of the Information Security Officer. Likewise, new system networks must not be established unless such approval has first been obtained. This process helps to ensure that all County of Humboldt systems have the controls needed to protect other network-connected systems.

Participation in external networks as a provider of services that external parties rely on is expressly prohibited unless three (3) conditions are first fulfilled. Specifically, the County Counsel's Office must identify the legal risks involved, the County Administrative Office must expressly accept any and all risks associated with the proposal, and the Information Technology Division must approve the network configuration and firewall.

Users initiating sessions via VPNs connected to County of Humboldt internal networks and/or multi-user computer systems must pass through an additional access control point (firewall) before users employing these lines can reach a log-in banner.

Unless approved in advance by the Information Security Officer, VPN connections that do not go through approved firewalls to reach County of Humboldt internal-network connected systems are prohibited.

Approved County employees and authorized third parties, such as visitors and vendors, may use VPNs. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to the County's internal networks. VPN use is to be controlled using either a one-time password authentication, such as a token device, or a public/private key system with a strong passphrase. VPN gateways will be set up and managed by the Information Technology Division [s1].

Remote maintenance ports for County of Humboldt computer and communication systems must be disabled until the specific time as they are needed by the vendor. These ports must then be again disabled immediately after use. The standard firewall access control is needed for an inbound connection.

The connection between County of Humboldt internal networks and the Internet, or any other publicly accessible computer network, must include an approved firewall and related access controls. This connection will be established and operated by the Information Technology Division for the entire County of Humboldt network. The establishment of a direct connection between County of Humboldt systems and computers at external organizations, via the Internet or any other public network, is prohibited, except as maintained by the Information Technology Division.

The connection between County of Humboldt internal networks and external networks maintained by the State of California must include an approved firewall and related access controls. The design of all connections shall include participation and approval by the Information Technology Division.

Portable phones using radio technology as well as cellular phones should not be used for data transmissions containing “confidential” or “restricted” County of Humboldt information unless the connection is encrypted. Likewise, other broadcast networking technologies, including, without limitation, radio-based local area networks, must not be used for these types of County of Humboldt information unless the link is encrypted. Such links may be used for electronic mail as long as the user understands that it contains no “confidential” or “restricted” information.

2.4 COMPUTER VIRUSES, WORMS, SPYWARE, AND TROJAN HORSES:

A computer virus is an unauthorized program that replicates itself, attaches itself to other programs, and spreads onto endpoint devices, data storage media, and/or across a network. The symptoms of virus infection include, without limitation, much slower computer response time, inexplicable loss of files, ransomware, changed modification dates for files, increased file sizes, and total failure of computers.

The connection of the County of Humboldt’s network to the Internet creates one (1) of the single highest risk points to the security of the County of Humboldt’s information systems. Since the Internet is a public network, there is always the potential for anyone for any reason to attempt to make unauthorized access to County of Humboldt information system resources to just look or to do damage. The resources and services available on the Internet must also be used with care by County of Humboldt staff.

All software downloaded from non-County of Humboldt sources via the Internet should be screened with virus detection software before being invoked. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone non-production machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

To assure continued uninterrupted service for computers and networks, all personal computer users should keep approved virus screening software enabled on their computers. This screening software should be used to scan all software coming from either third parties or other County of Humboldt departments; the scanning should take place before the new software is executed. Users may not bypass scanning processes that could arrest the transmission of computer viruses.

Users are responsible for immediately alerting their Departmental Manager or the Information Technology Division’s “help-desk-line” whenever they believe that a system has been infected with a virus. This will allow steps to promptly be taken to assure that no further infection takes place and that the technical staff needed to eradicate the virus is promptly engaged.

To assist with the post-virus-infection restoration of personal computer computing environments, all personal computer software should be copied before its initial usage, and such copies should be stored in a safe place. These master copies should not be used for ordinary business activities but should be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems. These master copies should also be stored in a secure location.

Larger systems do not generally suffer from viruses, but they do suffer from spyware, worms, Trojan horses, and ransomware. Worms are much like viruses but do not attach themselves to other programs. Trojan horses are unauthorized programs hidden within authorized programs. To prevent problems with viruses, worms, ransomware and Trojan horses, County of Humboldt computers and networks should not run software that comes from sources other than other government agencies, knowledgeable and trusted user groups, well-known systems security authorities, computer or network vendors, commercial software vendors, or developed by County of Humboldt staff or contractors. Software developed from untrusted sources must not be used unless it has first been subjected to a rigorous testing regimen approved by the Information Security Officer.

2.5 DATA AND PROGRAM BACKUP:

To protect County of Humboldt information resources from loss or damage, personal computer users are responsible for backing-up the information on their machines. For multi-user computer and communication systems, a system Administrator is responsible for making periodic backups.

If requested, the Information Technology Division will provide data and program backup services for departments. All sensitive, "confidential," "restricted," valuable, or critical information resident on County of Humboldt computer systems and networks should be periodically backed up. User department managers must define which information and which machines are to be backed up, the frequency of backup, and the method of backup. Recommended guidelines, include, without limitation, all of the following:

- Within departments with server-based user folders, it is recommended that all critical information be saved to the server-based user folder rather than the user's local drives. These folders should then be backed up for the department as a whole.
- If the system supports more than one (1) individual and contains data that is critical to the County of Humboldt's day-to-day operations, daily backup is recommended.
- If the system is used to support job-related functions and contains key data critical to the day-to-day operation of that job, weekly backup is recommended.
- If the system is primarily used as a personal productivity tool and contains no data that would be classified as job-related or departmental in-nature, backup frequency shall be at the discretion of the individual user.

Nothing in the timeframes for periodic backup set forth in this this Information Systems Policy restricts the generation of more frequent backups, as will occasionally be required for operational and business reasons.

For multi-user machines, whenever systems software permits, backups should be performed without user involvement, over an internal network and during the night.

Storage of backup media is the responsibility of the personal computer user or multi-user machine System Administrator involved in the backup process. Unless the information retention period is dictated by applicable local, state or federal, laws, regulations, polices, procedures or standards, information should be retained for as long as necessary but for no longer. Information subject to applicable local, state or federal, laws, regulations, policies, procedures or standards should be retained for the period specified. Other information should be destroyed when no longer needed, generally within two (2) years. The destruction of computer records should comply with the County of Humboldt's Retention Policy.

To prevent "confidential" and/or "restricted" County of Humboldt Information from being revealed to, or used by, unauthorized parties, all such information stored on a backup computer should be encrypted using approved encrypting methods, at the discretion of the Departmental Manager.

2.6 ENCRYPTION:

When "confidential" or "restricted" County of Humboldt information is transmitted over any external communication network, it should be sent in encrypted form. Likewise, whenever the County of Humboldt source code, or other source code that has been entrusted to the County of Humboldt by government agencies, vendors or other third parties, is to be sent over a network, it too should be in encrypted form.

Similarly, whenever “confidential” or “restricted” County of Humboldt information is not being actively used, it should be stored in encrypted form. This means that when “confidential” or “restricted” information is stored or transported in computer-readable storage media outside a secure area it should be in encrypted form.

When data is encrypted, it should be achieved via commercially-available products approved by the Information Security Officer.

Whenever encryption is used, users should not delete the sole readable version of the information unless they have first demonstrated that the decryption process can reestablish a readable version of the information.

Encryption keys used for County of Humboldt information are always classified as “confidential” or “restricted” information. Access to such keys must be strictly limited to those who have a need to access “confidential” or “restricted” information. Encryption keys should not be revealed to consultants, contractors, temporaries, or third parties without prior approval from the Information Technology Division Director. Likewise, encryption keys should always be encrypted when sent over a network.

Whenever such facilities are commercially available, the County of Humboldt should employ automated rather than manual encryption key management processes for the protection of information on County of Humboldt networks.

2.7 PORTABLE COMPUTERS:

Users in the possession of portable, laptops, notebooks, tablets, mobile phones, and other transportable computers containing “confidential” or “restricted” County of Humboldt information should not leave such computers unattended at any time unless the information is stored in encrypted form.

To prevent unauthorized disclosure, users in the possession of transportable computers containing unencrypted “confidential” or “restricted” County of Humboldt information should not check such computers in airline luggage systems, with hotel porters, etc. These computers should remain in the possession of the traveler as hand luggage.

Whenever “confidential” or “restricted” County of Humboldt information is written to a Universal Serial Bus (USB) flash drive or other storage media, the storage media should be suitably marked with the highest relevant sensitivity classification. When not in use, this media should be stored in a locked safe, locked furniture, or a similarly secured location.

2.8 REMOTE PRINTING:

Printers should not be left unattended if “confidential” or “restricted” County of Humboldt information is being printed or will soon be printed. The persons attending the printer should be authorized to examine the information being printed. Unattended printing is permitted if the area surrounding the printer is physically protected such that persons who are not authorized to see the “confidential” or “restricted” County of Humboldt information being printed may not enter.

2.9 PRIVACY:

Unless contractual agreements dictate otherwise, messages, including, without limitation, electronic mail (e-mail) messages and other forms of electronic correspondence, sent over County of Humboldt computer and communications systems are the property of the County of Humboldt. To properly protect and manage this property, the County of Humboldt reserves the right to examine all data stored in or transmitted by County of Humboldt computer and communications systems. Since County of Humboldt computer and communication systems are provided for business purposes, users should have no expectation of privacy associated with the information they store in or send through these systems.

Users should remember that e-mail messages can be forwarded, intercepted, printed, and stored so that they can be read by others, and at times may even have to be disclosed to outside parties or a court pursuant to the California Public Records Act or in connection with litigation. Therefore, it is in the best interests of all users that messages are professional, courteous, and businesslike.

When providing computer networking services, the County of Humboldt does not provide default message protection services such as encryption. Accordingly, no responsibility is assumed for the disclosure of information sent over County of Humboldt networks, and no assurances are made about the privacy of information handled by County of Humboldt internal networks. In those instances where session encryption or other special controls are required, it is the user's responsibility to make sure that adequate security precautions have been taken. Nothing in this paragraph should be construed to imply that this Information Systems Policy does not support the controls dictated by agreements with third parties, such as organizations that have entrusted the County of Humboldt with confidential, or other sensitive proprietary, information.

2.10 LOGS AND OTHER SYSTEMS SECURITY TOOLS:

Whenever cost-justifiable, automated tools for handling common security problems should be used on County of Humboldt computers and networks.

To the extent that systems software permits, computer and communications systems handling sensitive, valuable, or critical County of Humboldt information should securely log all significant security-relevant events. Examples of security-relevant events include, without limitation: users switching user-IDs during an on-line session; attempts to guess passwords or use privileges that have not been authorized; and modifications to production application software, system software, user privileges, and logging subsystems.

Logs containing County of Humboldt computer or communications system security-relevant events are important for error correction, security breach recovery, investigations, and other efforts, and should be retained, whenever possible, for at least six (6) months. During this period, logs should be secured such that they cannot be modified, and such that they can be accessed only by authorized persons.

To provide evidence for investigation, prosecution, and disciplinary actions, certain information should be captured whenever it is suspected that computer or network-related crime or abuse has taken place. The relevant information should be securely stored off-line for a minimum of two (2) or until it is determined that the County of Humboldt will not pursue legal action or otherwise use the information. The information to be immediately collected includes, without limitation, system logs, application audit trails, other indications of current system status, as well as copies of all potentially involved files.

To allow proper remedial action to be taken promptly, records reflecting security-relevant events should be periodically reviewed promptly by computer operations staff, information security staff, or systems administration staff.

Users must be put on notice about the specific acts that constitute computer and network security violations. Users must also be informed that such violations will be logged.

System Administrators are required to promptly apply all security patches to the operating system that have been released by: knowledgeable and trusted user groups; well-known systems security authorities; or the operating system vendor. Only those systems security tools supplied by such sources or by commercial software firms may be used on County of Humboldt computers and networks.

2.11 HANDLING NETWORK SECURITY INFORMATION:

From time to time, the Information Technology Division will designate individuals to audit compliance with this Information Systems Policy and other County of Humboldt computer and network security policies. At the same time, every user must promptly report any suspected network security problem, including, without limitation, intrusions and out-of-compliance situations, to the Information Security Officer or the Information Technology Division.

Computer viruses can spread quickly and need to be eradicated as soon as possible to limit serious damage to computers, networks, and County of Humboldt information. Accordingly, provided no intention to damage County of Humboldt systems existed, if users report a computer virus infestation immediately after it is noticed, even if their negligence was a contributing factor, no disciplinary action will be taken.

All network or systems software malfunctions should be immediately reported to the Information Security Officer, or Information Technology Division, or the involved external information system service provider. Ignoring such malfunctions could lead to serious problems such as lost or damaged information as well as unavailable network services.

Information about security measures for County of Humboldt computer and communications systems is confidential and must not be released to people who are not authorized users of the involved systems unless the permission of the Information Technology Division Director has first been obtained.

2.12 PHYSICAL SECURITY OF COMPUTER AND COMMUNICATIONS GEAR:

All County of Humboldt network equipment should be physically secured with anti-theft devices if located in an open office environment. Additional physical access control may also be used for such devices. For example, local area network servers should be placed in locked cabinets, locked closets, or locked computer rooms.

Access to systems development staff offices, telephone wiring closets, computer machine rooms, network switching rooms, and other County of Humboldt work areas containing “confidential” or “restricted” information should be physically restricted. Management responsible for the staff working in these areas should consult the Information Technology Division to determine the appropriate access control method, which include, without limitation, receptionists, metal key locks, and magnetic card door locks.

All users who must keep “confidential” or “restricted” County of Humboldt information at their homes shall have lockable furniture for the proper storage of such information. At the time of separation from the County of Humboldt, both the “confidential” or “restricted” information and the furniture used to store such information, if supplied by the County of Humboldt, must be immediately returned.

“Confidential” or “restricted” County of Humboldt information should not be downloaded to remote locations unless proper physical security and encryption facilities are installed and faithfully observed.

County of Humboldt Computer systems and communications equipment should be installed in a manner that is designed to protect such equipment during natural disasters, including, without limitation, earthquakes, floods, and fires.

2.13 PUBLIC REPRESENTATIONS:

Users may indicate their affiliation with the County of Humboldt in on-line forums, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words to a username or other identification method, or it may be implied via an e-mail address or other circumstances. In either case, whenever users provide an affiliation, they must also clearly indicate the opinions expressed are their own, and not necessarily those of the County of Humboldt. All external representations on behalf of the County of Humboldt should first be cleared with the user's Departmental Manager.

2.14 UNACCEPTABLE USES:

Users cannot utilize County of Humboldt computers or network systems to harass or defame anyone in any manner. Harassment of any kind is unacceptable. Messages that disclose personal information, without authorization, are also prohibited.

Although this is not an all-inclusive list, **users should be prohibited from the following unacceptable use of systems:**

- Use systems including E-mail to communicate sexual or other harassment. Include words or phrases that may be construed as derogatory based on race, color, sex, age, disability, national origin, or any other category.
- Any attempt to negate or circumvent security controls, policies and procedures (e.g., disabling virus protection or tunneling a protocol through a firewall).
- Unauthorized use, destruction, modification, and distribution of information or information systems.
- Sabotage, destruction, misuse, or unauthorized system repairs on information systems.
- Use of personal computing systems or test devices within or on networks without the written permission of management.
- Removal of any equipment (with the exception of authorized laptops) or software prior approval has been obtained.
- Use information systems to solicit for commercial ventures, religious or political causes, or for personal gain.
- Use of tools that compromise security (e.g., password crackers and network sniffers).
- Theft of resources including sensitive information.
- Use that violates local, state or federal laws.

2.15 COUNTY INTERNET WEB DEVELOPMENT STANDARDS:

All web page development for the County of Humboldt website must conform to the Humboldt County Website Accessibility Policy.

2.16 Electronic Meeting Usage:

Any and all applicable local, state and federal laws, regulations, and standards, including, without limitation, the California Brown Act, the California Public Records Act, the California Information and Practices Act of 1977, the California Confidentiality of Medical Information Act, the United States Health Information Technology for Economic and Clinical Health Act, and the United States Health Insurance Portability and Accountability Act of 1996, as well as any and all policies and procedures implemented by the Information Technology Division, all as may be amended from time to time, shall apply to the use of web-based conferencing services such as Zoom, Webex, and others.

The following guidelines shall be followed, regardless of which web-based conferencing service is used to facilitate internal or external meetings:

- Avoid using public hotspots and networks without VPN enabled. Use VPN to mitigate risks.
- Keep current and ensure users are using the updated version of remote access/meeting applications.
- Change passwords on a regular basis.
- Do not make meetings or classrooms public. Teleconferencing software often has options to make a meeting private. The most common options are to require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screen sharing options. Where possible, change screen sharing to “Host Only.”
- When recording, it is the responsibility of the user to make all attendees aware in advance of any conference being recorded.
- Adhere to any telework policy requirements for physical and information security enacted by the County of Humboldt.

Section III Use of Personal Computers:

3.1 GENERAL SECURITY:

- County of Humboldt data, computers, information, and communications systems and networks are provided for County of Humboldt purposes.
- An employee or contractor may be permitted to bring a “personally-owned” personal computer or any of its parts into the workplace. Use of such equipment with County of Humboldt information systems or data is permitted only after permission has been granted by the Departmental Manager and Information Security Officer.
- Users of the County of Humboldt personal computers need to review information security procedures annually.

3.2 STANDARDS:

All County of Humboldt personal computers must comply with hardware and software configuration standards approved by the Information Security Officer and the Information Technology Division Director.

3.3 HARDWARE SECURITY:

- Eating or drinking while using a personal computer system is strongly discouraged.
- To the extent possible, personal computers should be protected against environmental hazards such as electromagnetic radiation, dust, fire, and water leaks.
- An approved in-house standard electrical uninterrupted power supply should be installed to

protect all personal computer systems. Personal computers used for production business applications should also employ approved uninterruptible power systems.

- Personal computer equipment should be physically protected to lessen the risks of theft, destruction, and/or misuse. Suggested techniques to lessen these risks include, without limitation, housing the equipment in a locked room, physically locking the equipment to its workstation, or providing guard service or other physical security to protect the premises containing personal computers.

- Each piece of personal computer equipment should be marked for identification, inventory control, and insurance coverage. Inventory records of personal computer equipment must be kept up-to-date. All copies of inventory changes shall be provided to the Information Technology Division in order to allow for updating of the master inventory.

- Personal computer equipment should not be moved or relocated without the prior approval of the Departmental Manager.

- Anyone seeking to remove personal computer system equipment from a County of Humboldt office should obtain written authorization from the Departmental Manager. Portable computers brought into, and/or taken out of, County of Humboldt offices, no matter who owns them, should also have such authorization.

- The loss or theft of any personal computer hardware and/or software should be reported immediately to the Departmental Manager and the Information Technology Division. Upon verification that the equipment has not been removed by authorized County of Humboldt staff, a police report must be filed. The Humboldt County Director-Human Resources/Risk Manager shall be notified and provided a copy of the police report.

- To prevent unauthorized access, users should configure their screen savers to blank the screen and require a password to resume whenever their workstations are unattended for more than the time established in this Information Systems Policy or by the Departmental Manager whichever is shorter. If sensitive information resides on personal computers, screen savers should be manually invoked whenever users leave such personal computers.

- Personal computer systems that handle sensitive information should employ an approved access control mechanism (e.g., software or hardware) to restrict access to authorized users.

3.4 SOFTWARE SECURITY:

- Unless they receive information to the contrary, users should assume that all software on County of Humboldt personal computers is protected by copyright. Software purchased by the County of Humboldt should be used in accordance with any and all applicable contractual requirements and copyright laws.

- Commercial personal computer software purchased by the County of Humboldt is authorized for County of Humboldt use only. Making copies of County of Humboldt purchased software for personal use is illegal and prohibited, unless the software manufacturer has included in their copyright an allowance for use of the software on a home computer to perform work-related tasks at home. Any and all copying of software purchased by the County of Humboldt shall receive prior authorization by the Departmental Manager.

- Regardless of the type of software license that County of Humboldt has purchased, users should not copy, modify, or transfer software without the prior approval of the Departmental

Manager.

- Software authorized for use on County of Humboldt personal computers is that which has been purchased through the normal requisition procedures or has been developed by County of Humboldt employees or contractors. Use of unauthorized software, including, without limitation, software that has been borrowed or purchased by the user, is strictly prohibited. Freeware, shareware, and other software obtained without cost are considered unauthorized, unless specifically approved for use by the Information Technology Division Director.

- No modifications may be made to software resident on County of Humboldt personal computers without the prior consent of the System Administrator. Changing computer program parameters, like margins in a word processing package, is not considered to be a software modification.

- It is recommended that approved virus screening programs should be enabled on all personal computers at all times.

- If a virus detection program indicates that a virus has been discovered, the involved users must immediately notify the Departmental Manager or Information Technology Division. Users must not attempt to eradicate a virus or otherwise use the affected machine(s) until authorized personnel have addressed the problem.

- Externally supplied storage media should not be used on any County of Humboldt personal computer unless this storage media has first been checked for viruses and has been marked that no viruses were found.

- All end-user programming that results in a production business application system should be documented according to current Information Technology Division standards. A production system is a system used to process actual business transaction data.

- When a personal computer is used as the primary machine supporting one (1) or more production business applications, this machine should run an approved access control system that provides privilege control as well as change control.

3.5 DATA SECURITY:

- Users are required to delete sensitive information when such information is no longer needed or useful.

- Defective or damaged USB flash drives or external hard drives with sensitive information should be destroyed according to methods approved by the Departmental Manager.

- Sensitive information printed on hardcopy output should be shredded before disposal.

- Sensitive information displayed on a personal computer screen should be protected from unauthorized viewing via screen saver programs, access control programs, and the arrangement of office furniture.

- Sensitive information may not be removed from County of Humboldt offices or premises without the advance approval of the Departmental Manager. This requirement is particularly relevant to those who use portable computers.

- Sensitive information should be electronically erased before the media leaves the County of Humboldt’s possession or control.

- Whenever possible, sensitive information should be removed from personal computers and hard drives before they are sent out for repair. If this is not possible, personal computers and hard drives containing sensitive, "confidential," or "restricted" information shall repaired only by vendors with whom a nondisclosure agreement has been executed. Alternatively, personal computers and hard drives containing sensitive, "confidential," or "restricted" information may be repaired on-site under the supervision of an authorized County of Humboldt employee or vendor.

- Before separating from the County of Humboldt, upon a supervisor's request, users must provide all data stored on their laptop, workstation, and other endpoint devices. A user may not take any sensitive information away from the County of Humboldt upon separation unless prior written permission has been obtained from the Departmental Manager. All assigned user-IDs must be revoked during the pre-exit clearance process. All hardware and software on loan to the user must be returned to the appropriate County of Humboldt office.

- Before a County of Humboldt personal computer is transferred from department to another department, the hard drive must be completely erased.

3.6 GENERAL PROCEDURES:

Consistent with generally accepted business practice, the County of Humboldt collects statistical data about electronic communications. Using such information, technical support personnel monitor the use of electronic communications to ensure the ongoing availability and reliability of these systems.

Any and all Data, especially e-mails, no longer needed for business purposes should be periodically purged by users from their electronic message storage areas. After a two (2) year period, electronic messages backed-up to a separate data storage media will be deleted at the discretion of systems administration staff. Not only will this process increase scarce storage space, but it will also simplify records management and related activities.

Section IV Definition of Terms:

Access control: A system which restricts the activities of users and processes on a need-to-know basis.

Agents: Software that performs special tasks on behalf of a user, such as searching multiple databases for designated information.

Algorithm: A mathematical process for performing a certain calculation; generally used to refer to the process for performing encryption.

Badge reader: A device that reads badges and interconnects with a physical access control system.

Booting: The process of initializing a computer system from a turned-off state.

Bridge: A device that interconnects networks or that otherwise allows networking circuits to be connected.

Cipher lock: A device that requires the entry of passwords at doors and provides physical access control over a room or building.

Compliance statement: A document used to obtain a promise from a computer user that such user will abide by system policies and procedures.

Confidential information: A designation for information, the disclosure of which is expected to damage the County of Humboldt or its business affiliates (see restricted information).

Critical information: Any information essential to the County of Humboldt's business activities, the destruction, modification, or unavailability of which would cause serious disruption to the County of Humboldt's business.

Cryptographic challenge/response: A process for identifying computer users involving the issuance of a random challenge to a remote workstation, which is then transformed using an encryption process, and a response is returned to the connected computer system.

Default file permission: Access control file privileges, including, without limitation, read, write, and execute privileges, granted to computer users without further involvement of either System Administrators or users.

Default password: An initial password issued when a new user-ID is issued, or an initial password provided by a computer vendor when hardware or software is first delivered.

Downloading: The transfer of data from a host computer system, including, without limitation, mainframes, minicomputers, and network servers, to a connected workstation, such as a personal computer.

Dynamic password: A password that changes each time a user logs-into a computer system.

Encryption key: A secret password or bit string used to control the algorithm governing an encryption process.

Encryption: A process involving data coding to achieve confidentiality, anonymity, time-stamping, and other security objectives.

End-user: A user who employs computers to support the County of Humboldt business activities, who is acting as the source or destination of information flowing through a computer system.

Extended user authentication technique: Any procedure used to bolster the user identification process achieved by user-IDs and fixed passwords (see hand-held tokens and dynamic passwords).

Extranet: A private network that uses the Internet protocols and the public telecommunication system to share a business's information, data or operations with external suppliers, vendors or customers. An extranet can be viewed as the external part of a company's Intranet.

Firewall: A logical barrier stopping computer users or processes from going beyond a certain point in a network unless such users or processes have first passed some security check, such as providing a password.

Front-end telecommunications processor: A small computer used to handle communications interfacing, including, without limitation, polling, multiplexing and, error detection, for another computer.

Gateway: A computer system used to link networks that restricts the flow of information and employs some type of access control method.

Information retention schedule: A formal listing of the types of information that must be retained for archival purposes and the timeframes that such information must be kept.

Internet: A worldwide system of computer networks in which any one (1) computer can get information from, or talk to, any other connected computer using the Transmission Control Protocols/Internet Protocols.

Intranet: A private network inside a company or organization which uses the same kinds of software thatare found on the public Internet, but only for internal use.

Isolated computer: A computer which is not connected to a network or any other computer such as a stand-alone personal computer.

Log-in banner: The initial message presented to a user when first making a connection with a computer.

Log-in script: A set of stored commands which can log a user into a computer automatically.

Master copies of software: Copies of software that are retained in an archive and not used for normal business activities.

Multi-user computer system: Any computer which can support more than one (1) user simultaneously.

Password guessing attack: A computerized or manual process whereby various possible passwords are provided to a computer to gain unauthorized access.

Password reset: The assignment of a temporary password when a user forgets or loses his or her password.

Password-based access control: Software that relies on passwords as the primary mechanism to control system privileges.

Password: Any secret string of characters used to positively identify a computer user or process.

Personal computer: A general-purpose or portable computer, including, without limitation, laptops, tablets, and smartphones, consisting of one (1) or more microprocessors assembled in a unit. The unit typically consists of a central processing unit, video display, keyboard, disk drive, and several peripheral devices.

Identification: The process of definitively establishing the identity of a computer user.

Privilege: An authorized ability to perform a certain action on a computer, such as accessing a specific computer file.

Privileged user-ID: A user-ID that has been granted the ability to perform special activities, such as shutting down a multi-user system.

Restricted information: Particularly sensitive information, the disclosure of which is expected to severely damage the County of Humboldt or its business affiliates (see confidential information).

Router: A device that interconnects networks using different layers of the Open Systems Interconnection Reference Model.

Screen saver: A computer program that automatically blanks the screen of a computer monitor or CRT after a certain period of no activity.

Hand-held token: A commercial dynamic password system that employs a smart card to generate one-time passwords that are different for each session.

Security patch: A software program used to remedy a security or other problem commonly applied to operating systems.

Sensitive information: Any information, the disclosure of which could damage the County of Humboldt or its business associates.

Software macro: A computer program containing a set of procedural commands to achieve a certain result.

Special system privilege: Access system privileges allowing the involved user or process to perform activities that are not normally granted to other users.

Suspending a user-ID: The process of revoking the privileges associated with a user-ID.

System Administrator: A designated individual who has special privileges on a multi-user computer system in order to monitor security and other administrative matters.

Terminal function keys: Special keys on a keyboard that can be defined to perform certain activities, such as saving a file.

Uploading: The transfer of data from a connected device, such as a personal computer, to a host system, such as mainframes and minicomputers.

User-IDs: Character strings that uniquely identify computer users or computer processes which are also know as accounts.

Valuable information: Information of significant financial value to the owner thereof.

Verify security status: The process by which controls are shown to be both properly installed and properly operating.

Virus screening software: Commercially-available software that searches for certain bit patterns or other evidence of computer virus infection.

Virtual Private Network: The process for using the internet or other public carriers as transit for private network traffic in a secure encrypted form.