County of Hawai'i

Department of Information Technology

Employee Policies

County of Hawai'i

Electronic Resources Policy

Date: December 30, 2016
Revised: July 1, 2017
Revised: March 23, 2020

Purpose:

The purpose of this policy is to establish acceptable use of computer and electronic resources provided to the agents and employees of the County of Hawai'i (County) and to encourage proper usage. This shall also serve as a reminder that materials produced using County resources while under County employment, contract or assignment is the property of the County of Hawai'i and the County asserts its proprietary interest therein. This policy shall also apply to any other organization(s) or individual(s) that is (are) granted use of the equipment and resources.

Procedure:

A. Background

The County provides Internet, Networks, Information Systems, E-mail, and electronic devices to agents and employees to transact County Business. These devices and services are County property, the purpose of which is to facilitate County business, and as such, their use is subject to County scrutiny, control and policy. These devices and services are provided to individual employees or agents at the discretion of the County and are a revocable privilege.

B. Internet Security

Although the Internet has provided the opportunity for information exchange among millions of users, it is currently unsecured and unregulated. It provides opportunities for unauthorized access to other connecting networks, illegal penetration of systems by "hackers," fraudulent data manipulation, introduction of computer viruses, and many other security-related problems.

Therefore, it is mandatory that each employee using County devices or approved personal electronic devices to access the Internet and/or e-mail must take proper precautions to protect the County's devices, network, and information systems from unauthorized access, damage, and tampering.

Those accessing the Internet and e-mail from the County network via County electronic devices or County approved personal electronic devices, should have no expectation of privacy.

C. Guidelines

I. Access

a. Department Heads (or their designated alternatives) may request via the Department of Information Technology (DIT) Computer Access Request Form (CARF) for individual agents and employees to have access to the Internet, E-mail, and other systems through the County's networks, certifying that said employee has a business need for such access. Access request for Agencies not supported by DIT may have different request procedures.

b. Access to the Internet from the County's network shall only be via software approved by DIT using County owned and/or approved personal electronic devices.

c. Access to the County Network will require end-user cyber-security training and assessments. Training will be provided initially for all new users. Through ongoing assessments, training will also be targeted to high-risk end users identified through phishing campaigns.

II. Usage

Employees or agents may make occasional, incidental, personal use of the Internet and/or e-mail in accordance with this policy and their respective department's internal office policies.

A. Individual employees are responsible for the appropriateness and content of material they create, transmit and/or access via the County's network and systems. Prohibited uses include, but are not limited to, the following:

- Using someone else's account
- Leaving computer logged in with your credentials unlocked in a physically unsecure location or allowing anyone to access systems in your name
- Masking the identity of an account or machine
- Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, or deleting without explicit agreement of the owner
- Commercial for-profit purposes (financial) or personal gain
- Streaming of audio or video for personal entertainment
- Religious causes or political lobbying
- Engaging in disruptive or malicious activities such as unauthorized software, hardware, or data modification
- Intentional creation and/or propagation of a computer virus, trojan horse, worm or malware
- For hate mail, harassment, or discriminatory purposes
- For installing or downloading any software not approved and/or licensed to the County
- Online gambling
- Accessing material with pornographic or sexual content
- Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy

B. Engaging in prohibited Internet usage as noted above may result in disciplinary actions up to and including discharge by the Employer for just and proper cause.

C. This entire policy applies during work and non-work hours.

D. Enabling remote access to the Virtual Private Network (VPN), on-premise or any cloud-based County application or other County system shall not constitute or imply the expectation or approval of any employee to perform work outside of their normal work hours. The performance of any work outside of normal work hours shall be subject to the respective department's overtime standard operating procedure and supervisor approval

E. Email Blasts. Employees and agents are prohibited from sending organization wide email messages to all employees and agents without approval from the Mayor's Office. Employees and agents are prohibited from sending email blasts, (mass mailings) to external parties without approval from the Mayor's Office. Only the Director of Information Technology, Systems Support, or User Support Manager and/or authorized Systems Administrators may generate public email distribution lists (email blasts). Employees and agents are prohibited from

requesting email replies to organization-wide email or external email blasts without permission from the Mayor's Office. All approved mass mailings must utilize the Bcc: field for email recipients to protect email address privacy as well as prevent accidental reply to all addresses in the mass mailing.

III. Monitoring

The County will not monitor e-mail messages as a routine matter. There may be a need, however, for the County to occasionally review e-mail, Internet access, and/or electronic device content for a specific business or law enforcement reason. Communications to and from the Office of the Corporation Counsel and the Office of the Prosecuting Attorney protected by attorney-client privilege shall not be subject to monitoring in any form.

Users of personal electronic devices need to be aware that personal data is subject to review should there be a business or law enforcement reason to do so.

Therefore, there should be no expectation of privacy regardless of the device being used.

The County may further monitor general usage patterns of the Internet and e-mail to assure resources are devoted to maintaining the highest levels of business productivity.

IV. Security

In the event that a County-owned or personal electronic device is lost or stolen, for security purposes it may be necessary to remotely erase all data from the device. It may also be necessary to erase County data from a device should an employee leave service with the County.

This will result in the loss of all data including personal data on personal electronic devices. The County will not be responsible for the loss of personal data should a security erase be required.

V. Authorization for Review

A written request for review of a user's internet usage and/or email messages shall be made by the Department Head and subject to approval by the Director of the DIT. In reviewing such requests, the Director of the DIT shall consult with Corporation Counsel and the Director of Human Resources, as appropriate. Upon approval, a Systems Analyst in the DIT will provide the necessary information, files, e-mail, and/or log files to the Director of the DIT to complete the review with the Department Head.

Non-Compliance:

Any use contrary to this policy shall be reported to the non-compliant user's Department Head for appropriate action. Non-compliance with this policy may result in discipline up to and including dismissal in accordance with applicable rules, laws, and the appropriate collective bargaining agreement.

Exemption:

The Hawai'i Police Department (HPD) is exempt from this Policy. HPD maintains their own Policy that addresses similar risks. Exemptions are made at the discretion of the Police Chief.

The Hawai'i Police Department will administer and track the end-user cyber-security training and assessments required by the County of Hawai'i Department of IT for Hawai'i Police Department Personnel.

Distribution and Effective Date:

This policy shall be distributed and made available to every County employee who uses County owned electronic devices and/or that has access to the County Internet, networks, and E-mail system via County approved personal electronic devices.

Employees and agents shall acknowledge receipt and their understanding of the policies by their e-signature or wet signature on a separate acceptance page. The signature page shall be maintained for the record by the DIT, HR, or respective Department.

The County reserves the right to change these policies at any time, with such prior notice, if any, as may be reasonable under the circumstances.

Approved by:

Harry Kim, Mayor
County of Hawai'i

Aaron Chung, Council Chair
County of Hawai'i

County of Hawai'i

Password Policy

Effective Date: December 30, 2016
Revised: July 1, 2017
Revised: March 23, 2020

Purpose

Employees and agents at the County of Hawai'i must access a variety of IT resources, including computers and other hardware devices, data storage systems, and other accounts. Passwords are a key part of an IT security strategy to make sure only authorized people can access those resources and data.

All employees or agents who have access to any of those resources are responsible for choosing strong passwords and for protecting their log-in information from unauthorized people.

The purpose of this policy is to make sure all County of Hawai'i resources and data receive adequate password protection. The policy covers all employees and agents who are responsible for one or more account or have access to any resource that requires a password.

Password creation

- All passwords should be reasonably complex and difficult for unauthorized people to guess. Employees and agents must choose passwords that are at least eight characters long and contain at least 3 of the following 4 items: upper- and lower-case letters, numbers, and punctuation marks and other special characters. These requirements will be enforced with software when possible.
- In addition to meeting those requirements, employees and agents should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa$$w0rd" are equally bad from a security perspective. The password cannot contain the username or a portion of the username.
- A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization. For example, the phrase "This may be one way to remember" can become "TmB0WTr!".
- Employees and agents must choose unique passwords for all of their County accounts, and may not use a password that they are already using for a personal account.

- All passwords must be changed regularly and will expire every 90 days. This requirement will be enforced using software when possible. The system will remember the last 10 passwords used, meaning a password cannot be re-used until there have been 10 different previous passwords.
- Passwords can only be changed 1 time per 24-hour period without assistance from your support staff
- Default passwords — such as those created for new employees and agents when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.

Protecting passwords

- Employees and agents may never share their user accounts and passwords with anyone else in the County, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique user account and password.
- Employees and agents may never share their user accounts and passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.
- Employees and agents should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. All Employees and agents will receive training on how to recognize these attacks.
- Employees and agents must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.
- Employees and agents may not use password managers or other tools to help store and remember passwords without permission from their IT support.
- Advanced Authentication may be required for those users accessing Criminal Justice Information System ("CJIS") level security data/resources.

Approved by:

Harry Kim, Mayor
County of Hawai'i

Aaron Chung, Council Chair
County of Hawai'i

County of Hawai'i

Email Retention Policy

Effective Date: December 30, 2016
Revised: July 1, 2017
Revised: March 23, 2020

Purpose:

The purpose of this policy is to improve the management of limited electronic storage resources on the County's email servers while maintaining sufficient aging of emails for reference by users. This policy applies only to all ***deleted*** emails centrally stored on the County of Hawai'i's email servers.

Policy:

Deleted emails will be retained on the central County of Hawai'i email servers no longer than 90 days. Once emails deleted by the user have reached the 90-day retention threshold, the Information Systems Department will permanently remove them from the County's email server and they can no longer be retrieved.

Duty to Retain Government Records:

This email retention policy in no way changes the responsibility of departments follow the County's Paper and Electronic Records Retention Schedule (RRS). If the content of an email message is listed in the RRS as a record which must be retained for a specified period of time, then a copy of the email must be retained by the employee who has custody of the record.

Users requiring email storage are encouraged to retain those emails in some location other than the County's email servers. Examples of more appropriate ways to retain emails include 1) archiving or saving the email to the user's local computer or network storage, 2) copying the email to a CD or 3) creating a paper copy.

Approved by:

Harry Kim, Mayor
County of Hawai'i

Aaron Chung, Council Chair
County of Hawai'i

County of Hawai'i

Electronic Data Storage Destruction Policy

Effective Date: December 30, 2016
Revised: July 1, 2017
Revised: March 23, 2020

Purpose

The purpose of this document is to set forth a policy and procedure on the proper disposal of electronic data storage, be it in the form of magnetic floppy, magnetic tape, disk drives or USB sticks.

All electronic media must be destroyed to prevent access to any data on the media. Destruction can be in the form of crushing or shredding. The Department of Information Technology (DIT) has equipment designed to crush and destroy electronic media as well as a procedure to document the processing and destruction. To request assistance, please Contact DIT via email to help@hawaiicounty.gov.

Electronic Media Storage

Hard drives should be removed from PC's and laptops that are being recycled. A log of the system from which the drive was removed from and the date that the media was destroyed must be maintained. Upon completion of the crushing of the hard drive, the PC or Laptop can be removed from inventory and properly recycled.

Magnetic Media such as Floppy or Tape

This media can be rendered unusable by shredding or by cutting into pieces with scissors or shears.

USB Devices, Cell Phones, PDAs, etc.

This media should be crushed and disposed of.

Approved by:

Harry Kim, Mayor
County of Hawai'i

Aaron Chung, Council Chair
County of Hawai'i

County of Hawai'i

Mobile Device Policy

Effective Date: December 30, 2016
Revised: July 1, 2017
Revised: March 23, 2020

Introduction

Mobile devices, such as smartphones and tablet computers, are important tools for the organization and supports their use to achieve business goals. However, mobile devices also represent a significant risk to data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the County data and IT infrastructure. This can subsequently lead to data leakage and system infection. As a requirement to protect its information assets in order to safeguard its customers, intellectual property and reputation, this document outlines a set of practices and requirements for the safe use of mobile devices and applications.

Scope

1. All mobile devices, whether owned by employer or owned by employees and agents, inclusive of smartphones and tablet computers, that have access to County networks, data and systems are governed by this mobile device security policy. The scope of this policy does not include County IT-managed laptops.

2. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements, or if a department's policies are more restrictive) a risk authorized by security management must be conducted. The Office of the Corporation Counsel, the Office of the Prosecuting Attorney, and the Hawai'i Police Department have circumstances that require release from this Mobile Device Policy. Exemptions are made at the discretion and direction of the Corporate Counsel, Prosecuting Attorney, or Chief of Police respectively before any data is accessed or deleted.

3. Only devices managed by IT will be allowed to connect directly to the internal County network. These devices will be subject to the valid compliance rules on security features such as encryption, password, key lock, etc. These policies will be enforced by the IT department using Mobile Device Management software.

4. Technical support provided by the County for mobile devices owned by employee, referred to herein as Bring Your Own Device ("BYOD") will be limited to assistance in configuring the device to send and receive County email. If the BYOD device is not functioning correctly or cannot be connected to the County network, it is the responsibility of the employee to correct the technical malfunction of the device.

User Requirements

1. Users may only load County data that is essential to their role onto their mobile device(s).
2. Users must report all lost or stolen devices to their department immediately.
3. Devices must not be "jailbroken" or "rooted"* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
4. User MUST password protect their device, whether it is a BYOD or employer provided device to protect County data.
5. Users must not load pirated software or illegal content onto their devices.
6. Applications must only be installed from official platform-owner approved sources. Installation of code from untrusted sources is forbidden. If you are unsure if an application is from an approved source contact your department.
7. Devices must be kept up to date with manufacturer or network provided patches. As a minimum, patches should be checked for weekly and applied at least once a month.
8. Devices must not be connected to a PC which does not have up to date and enabled anti-malware protection and which does not comply with County policy.
9. Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that County data is only sent through the County email system. If a user suspects that County data has been sent from a personal email account, either in body text or as an attachment, the user must notify IT immediately.
10. The above requirements will be checked regularly. Should a device be noncompliant, it may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe.
11. The user is responsible for the backup of their own personal data and the County will accept no responsibility for the loss of files due to a non-compliant device being wiped for security reasons.
12. Users must not use County workstations to backup or synchronize device content such as media files, unless such content is required for legitimate business purposes. Users will not modify a mobile device to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software. Such actions will result in a full or partial wipe of the device by IT.

Approved by:

Harry Kim, Mayor
County of Hawai'i

Aaron Chung, Council Chair
County of Hawai'i

County of Hawai'i

Social Media Policy

Effective Date: December 30, 2016
Revised: July 1, 2017
Revised: March 23, 2020

I. Background

The use of social media has grown dramatically in recent years. Social media may be used positively to increase access to information and enhance social relationships. Social media may also be used negatively to violate individuals' privacy rights, disclose confidential information and spread incorrect information. Social media may also be used detrimentally to bully and harass others.

II. Scope

All officers, employees, and agents are subject to, and shall comply with, this Social Media Policy ("Policy") regarding personal use of social media.

III. Policy Statement

The use of social media by officers, employees and agents shall conform to this Policy and shall comply with all other policies, rules and directives as well as County, State and Federal laws.

IV. Definitions

"Social media" means all ways of communicating or posting information or content of any sort on the Internet, including, but not limited to, posting to one's own or to another entity's personal websites, blogs, social networking or affinity websites, web bulletin boards or chat rooms.

"County resources" means any property or information that is owned by the County or paid for with County funds, including, but not limited to, County-issued electronic equipment (e.g., laptop computers, desktop computers, smartphones, tablets, etc.), County paid time, e.g. hours and wages, and County email addresses.

V. Prohibited Conduct

A Use of Personal Social Media Accounts by Persons Subject to This Policy

1 The activities of persons subject to this Policy shall comply with all applicable County policies, rules, and directives, as well as all County, State and Federal laws. Applicable County policies, rules, directives and laws include, but are not limited to:

a Electronic Resources Policy,

b Violence in the Workplace Policy,

c Anti-Discrimination and Harassment Policy, and

d Hawai'i County Code Chapter 2, Article 15, Code of Ethics.

Employees and agents shall carefully read the documents noted above and ensure that their postings on social media conform to them.

2 The personal use of social media on County resources is prohibited.

3 Employees and agents shall not use their County e-mail addresses, County telephone numbers (including County-issued cellphone numbers) or any other County information (e.g., County mailing addresses) to register for and/or engage in the use of social networks, blogs, or other online accounts maintained for personal use.

4 Employees and agents shall not use their personal social media accounts for work or other County-related purposes.

5 Every employee and agent is solely responsible for all content that he or she posts online. Any personal use of social media that interferes with an employee's or agent's job performance or the performance of other employees and agents, or that adversely impacts customers, suppliers, or other agents who do work or volunteer for the County, may result in disciplinary action, up to and including discharge.

Volunteers and others who do work for the County and use social media for a negative or detrimental purpose against the County or its employees or agents may have their relationship with the County severed.

VI. Responsibilities

A The Department of Human Resources is responsible for updating this Policy as needed.

B Departments and Agencies are responsible to

1 Distribute this Policy to employees and agents,

2 Distribute acknowledgments of receipt of the Policy to employees and agents, collect signed receipts and file appropriately,

3 Communicate to employees and agents the type of information that is considered to be confidential including personal, County, departmental and/or agency information,

4 Ensure that employees and agents comply with this Policy, and

5 Timely and properly investigate possible violations and take appropriate and necessary action.

C Employees and agents are responsible to

1 Refrain from using personal social media accounts in a way that would violate this Policy, any other County policies and rules, State and Federal laws. Employees and agents who fail to comply with this Policy may face disciplinary action, up to and including discharge. Volunteers who fail to comply with this Policy may have their relationship with the County severed.

Exemption: The Office of the Prosecuting Attorney and the Hawai'i Police Department have circumstances that require release from this Social Media Policy. Exemptions are made at the discretion and direction of the Prosecuting Attorney or the Police Chief respectively.

Approved by:

Harry Kim, Mayor
County of Hawai'i

Aaron Chung, Council Chair
County of Hawai'i