

<b>STATE OF HAWAII DEPARTMENT OF HUMAN RESOURCES DEVELOPMENT POLICIES AND PROCEDURES</b>	POLICY NO. 103.001 DO/ISO	NO. of PAGES  15 1 Attachment
	EFF. DATE 05/25/04	REV.NO./Date Rev. No. 3 09/07/2017
TITLE:  <b>ACCEPTABLE USAGE OF IT RESOURCES</b>	APPROVED: <i>James K Nishimoto</i> James K. Nishimoto, Director	

**I. POLICY**

The use of the State's Information Technology (IT) resources by its employees is a privilege and shall be used for furthering State business and in service to the citizens of Hawaii. Usage shall be limited to legal purposes only. Usage shall not be for illegal, dishonest, disruptive, threatening, damaging to the reputation of the State, inconsistent with the mission of the State, or likely to subject the State to legal liability.

The primary subject matter expert for IT and lead agency for IT systems in State government is the Department of Accounting and General Services ("DAGS"), Office of Enterprise Technology Services ("ETS"). ETS participated in developing this policy and concurs with it, including its intent and the expectations placed on users of State IT resources.

**II. RATIONALE**

The State's IT resources are government property. As with other government property, employees are expected to limit usage of such resources to work-related activities and exercise care and caution when using this technology.

**III. PERIODIC REVIEW**

It is recommended that all departments in the executive branch should conduct periodic reviews of this policy document to ensure that their users are kept up to date with regards to new and additional policy requirements and to restate existing policy requirements. These periodic reviews shall remind users of their responsibility in the acceptable use of the state's IT resources and their obligation to protect the State's IT resources and to safeguard confidential agency resources, information, and data. Users will be required to re-sign the acknowledgement form once the periodic review has been completed.

**IV. DEFINITIONS**

"IT resources" means all hardware, software, documentation, programs, information, data, and other devices that are owned,

## ACCEPTABLE USAGE OF IT RESOURCES

**POLICY NO. 103.001 (Eff. 09/07/2017)**

leased or provided by the State. These resources include those that enable remote and local communication such as hubs, switches, routers, and concentrators or access between various platforms and environments such as the mainframe, minicomputers, servers, Local Area Networks ("LANs"), Wide Area Networks ("WANs"), and personal computers and mobile computing devices (e.g. laptops, notebooks, tablets, smartphone, etc.).

"Users" mean all State employees in the executive branch who are authorized to use or access the State's IT resources.

"Other Users" means volunteers, agents, contractors, consultants and other non-state users who are authorized to use or access the State's IT resources.

"Personal Data" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- (1) Social Security Number;
- (2) Driver's license number or Hawaii identification card number;
- (3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account;
- (4) Date of birth;
- (5) Home/cell/mobile phone and personal mail address.

Personal data also includes information described in Chapter 92F-14 and Chapter 487N of the Hawai'i Revised Statutes.

#### **IV. SCOPE**

This policy applies to all employees in the executive branch who are authorized to use or access the State's IT resources, excluding employees of the University of Hawaii and the Department of Education.

## ACCEPTABLE USAGE OF IT RESOURCES

**POLICY NO. 103.001 (Eff. 09/07/2017)**

Departments that permit volunteers, contractors, vendors, and members of the general public to access the department's IT resources shall be responsible for supervising and monitoring their usage and conduct.

### V. GENERAL PROVISIONS

#### A. PERMISSION AND ACCEPTANCE

By using or accessing the State's IT resources, the User accepts and agrees to all terms and conditions stated in this policy. In addition, all Users are required to sign Attachment A. Policy No. 103.001 ACCEPTABLE USAGE OF INFORMATION TECHNOLOGY RESOURCES ACKNOWLEDGMENT FORM, acknowledging that they received this policy, and understands and agrees to comply with the terms and conditions set forth in the document. Signoff on the acknowledgement form confirms that the User accepts and agrees to all the terms and conditions as contained in this policy. Users are also required to read all systems access NOTICE TO USERS, banners, warning messages, etc., before proceeding with any computer systems access. Continuing beyond these posted messages implies understanding and acceptance of the stated terms and conditions.

Departmental Human Resources Officers (HRO's) shall be responsible for informing all state personnel of their responsibility to the policy. Informing "Other Users" (as defined in section IV. Definitions), shall be the responsibility of the Director, Manager, Supervisor or designee granting access to state IT resources.

#### B. STATE AS OWNER, CUSTODIAN AND LICENSEE

The State, and not the employee, is the sole owner, custodian, and in cases of software, the licensed user of all IT resources.

#### C. NO EXPECTATION OF PRIVACY

Users are on notice that there is no proprietary interest and no reasonable expectation of privacy while using any of the IT resources that are provided by the State. The State considers all information and data processed, transmitted, received, and stored on the State's IT resources, including but not limited to,

## ACCEPTABLE USAGE OF IT RESOURCES

### POLICY NO. 103.001 (Eff. 09/07/2017)

processed documents, electronic and voice mail, and Internet communications as owned by the State. The State may obtain access to any of its resources at any time. The State may disclose any of its IT resources to law enforcement or other third parties without prior consent of the Users.

#### D. MONITORING AND ENFORCEMENT

The State is the owner or custodian of data and information that is stored on, processed by, or transmitted through the State's IT resources. The State may at any time, and without prior notice, monitor, audit, examine and/or disclose data and information such as the contents of electronic mail, individual file directories, access by users to Internet sites that are visited, blog entries, chat and/or news groups, downloaded or uploaded materials and other information for purposes such as, but not limited to, ensuring compliance with applicable rules, regulations, policies and procedures, monitoring the performance of the IT resources, and conducting investigations.

#### E. REVOCATION OF ACCESS TO IT RESOURCES

The State reserves the right, without advance notice to Users, to revoke access to IT resources, to override Users' passwords without notice, or to require Users to disclose passwords and/or codes to facilitate access to information that is processed and stored in the department's IT resources.

#### F. POLICY VIOLATION

Violation of this policy by Users may result in immediate revocation or curtailment of computer access and usage, disciplinary action that may include discharge from employment, and/or civil and criminal liability.

#### G. AMENDMENTS AND REVISIONS OF THIS POLICY

The State reserves the right to amend or revise this policy from time to time, as the need arises.

## ACCEPTABLE USAGE OF IT RESOURCES

POLICY NO. 103.001 (Eff. 09/07/2017)

### VI. RESPONSIBILITIES

#### A. DEPARTMENT OR AGENCY HEADS

##### 1. Development of Acceptable Use Policies

Department or agency heads may choose to develop and enforce their own IT acceptable use policies to further define the use of IT resources within their own departments or agencies. A sample *Acceptable Usage of Information Technology Resources Acknowledgment Form* is set forth as Attachment A.

Should a conflict exist, this *Acceptable Usage of Information Technology Resources* policy shall take precedence over all policies and/or procedures that are developed by the departments or agencies.

##### 2. Authorization and Supervision

Department or agency heads or their designees shall be responsible for:

- a. Authorizing the use of IT resources for specific users;
- b. Disseminating this policy and any amendments hereto;
- c. Ensuring that Users of IT resources are familiar with the provisions of this policy and any amendments hereto, including developing procedures to ensure that all affected employees are aware of this policy and any amendments hereto;
- d. Providing proper training to all departmental users having access to state IT resources;
- e. Supervising the use of IT resources, including taking reasonable precautions to safeguard the resources under their jurisdiction against unauthorized access, use, disclosure, modification, duplication or destruction;
- f. Ensuring that current and new Users are informed of appropriate uses of the State's IT resources;
- g. Enforcing this policy and any amendments hereto; and

## ACCEPTABLE USAGE OF IT RESOURCES

**POLICY NO. 103.001 (Eff. 09/07/2017)**

- h. Taking appropriate corrective action for violations of this policy and any amendments hereto.

### B. USERS' RESPONSIBILITIES

1. Familiarity with Policies

All Users shall become familiar with this and other supporting and applicable IT resource policies. Questions related to the applicability of this policy may be directed to the User's departmental personnel office. Questions related to the technical aspects of the IT resources may be directed to the User's departmental IT coordinator and/or departmental designated office.

2. Duty Not to Waste IT Resources

It shall be the Users' responsibility to:

- a. Not deliberately perform acts that waste IT resources or unfairly monopolize resources to the exclusion of others. Such acts include, but are not limited to, printing multiple copies of documents, using the e-mail system for sending mass mailings or chain letters, spending excessive amounts of time (unless it is in the course of work), on the Internet, engaging in online chat groups, or otherwise creating unnecessary network traffic;
- b. Not copy and/or download audio, video, and picture files, unless they are work-related; and
- c. Routinely delete outdated or otherwise unnecessary electronic communication and computer files to free up IT resources and help to keep systems running more efficiently and smoothly. Users shall be aware that the deletion of electronic communication and computer files may not fully eliminate the messages and files from the system. Users are directed to review the Department of Accounting and General Services "General Records Schedule" as well as any Department specific policy, which addresses deleting, erasing, discarding, or disposing of electronically stored information.
- d. Users are directed to review the Department of Accounting and General Services "General Records Schedule" as well

## ACCEPTABLE USAGE OF IT RESOURCES

**POLICY NO. 103.001 (Eff. 09/07/2017)**

as any Department, specific policy, which addresses deleting, erasing, discarding, or disposing of electronically stored information including email.

### 3. Duty to Act Lawfully, Ethically, Respectfully, and Responsibly

It shall be the Users' responsibility to:

- a. Act lawfully, ethically, respectfully, and responsibly in the use of the State's IT resources;
- b. Maintain the confidentiality of classified materials including personal data, financial data, and other proprietary and confidential state data;
- c. Transmit or disclose classified and/or confidential information including personal data, health data, financial data, and other proprietary and confidential state data, through secured electronic communication media only to another party who is authorized to receive or view such information; and
- d. Immediately report an encounter or receipt of unlawful, unethical, or questionable materials to a supervisor or the department or agency head's designee.

### 4. Duty to Protect the State's IT Resources

It shall be the Users' responsibility to:

- a. Take all reasonable precautions to protect the State's IT resources from unauthorized access, use, disclosure, modification, duplication, and/or destruction;
- b. Employ access controls, and other security measures provided by the department or agency and take prudent and reasonable steps to limit unauthorized access to IT resources;
- c. Assist and cooperate in the protection of the IT resources and follow departmental or agency procedures in matters such as, but not limited to, logging off and powering down while away from the computer and at the end of each workday, scanning files obtained from external sources

## ACCEPTABLE USAGE OF IT RESOURCES

**POLICY NO. 103.001 (Eff. 09/07/2017)**

for viruses or signs of other malicious codes prior to accessing the information, and making backup copies of files and data on the hard drives of their respective personal computers; and

- d. Not disclose passwords to any other individual (unless authorized to do so by the Department Director or delegated authority) as Users shall be held responsible for all computer transactions that are made with their user IDs and passwords.
- e. Passwords shall not be of the type that can be easily surmised, shall not be recorded where they may be easily obtained, and shall be changed immediately upon suspicion that an unauthorized person is aware of the User's password.
- f. Return all state property upon leaving state service as a result of transfer, termination, retirement, etc., including:
  - (1) Computer hardware, software, and peripheral devices, such as but not limited to monitors, CPU's, printers, USB drives, etc.
  - (2) Information and/or data including system documentation, logs, manuals, user guides, whether in electronic or hardcopy formats, on all media type, etc.,
  - (3) Means of access including systems and applications passwords, door keys, cypher lock combinations, etc.

### VII. PERSONAL USAGE

- A. Employees, in general, are permitted incidental and minimal personal usage of IT services and assets if such privilege does not adversely affect the program's operations or does not cause harm or embarrassment to the State, and does not consume excessive resources.
- B. Personal use of IT resources by an employee shall not interfere with his/her job duties or the operations of the State.
- C. Good judgment shall be exercised in using the State's IT resources.



## ACCEPTABLE USAGE OF IT RESOURCES

POLICY NO. 103.001 (Eff. 09/07/2017)

- D. An employee is not authorized personal use of IT resources that result in expenses or charges to the State and he/she shall not engage in the prohibited activities as described in Part VIII, *Prohibited Activities*, below. Employees shall be responsible for the payment of any charges and any additional cost that is incurred because of their personal use.
- E. Users who engage in personal use of the State's IT resources shall make it clear to all concerned that their activity or communication is not being sanctioned or used for official State business.

### VIII. PROHIBITED ACTIVITIES

The State explicitly prohibits all activities that are in violation of any

federal, State or other applicable laws, rules, regulations, and established policies and procedures. Such activities include, but are not limited to:

A. Unauthorized Access to Files and Directories

Users are strictly prohibited from:

1. Circumventing the security controls of the State's IT resources, including but not limited to, cracking other Users' passwords, decoding encrypted files, or using software application programs to secretly penetrate computer and information systems; and
2. Accessing directories and files of other Users in order to read, browse, modify, copy, or delete any data or information without the explicit approval of the individual User and/or the department or agency head or designee.

B. Unauthorized Use of Copyrighted or Proprietary

Materials Users are strictly prohibited from:

1. Illegally copying material that is protected under copyright law or from making such material available to others for copying;

## ACCEPTABLE USAGE OF IT RESOURCES

**POLICY NO. 103.001 (Eff. 09/07/2017)**

2. Illegally sending (uploading) material that is protected under copyright law, including trade secrets, proprietary financial information, or similar materials without the express prior

approval from the department or agency head or designee;  
and

3. Illegally receiving (downloading) material that is protected under copyright law, including trade secrets, proprietary financial information, or similar materials without the express prior approval from the department or agency head or designee.

Users who are unaware if the information is copyrighted, proprietary, or otherwise inappropriate for transfer, shall resolve all doubts in favor of not transferring the information and consult with their supervisor or the department or agency head or designee.

### C. Use of Hardware and Software, whether or not provided by the State

1. Users are strictly prohibited from installing hardware such as, but not limited to, communication cards, memory boards, video display adapters, other peripheral devices and modems, and software such as commercial, shareware, and freeware, on any computer system without the express approval of the department or agency head or designee.

2. Users are strictly prohibited from using, connecting, removing, performing, distributing or otherwise operating IT devices, systems. or services such as, but not limited to the following without prior written approval from the agency authority and signing the Acceptable Usage of IT Resources Acknowledgement Form (See Attachment A) by the User:

#### a. Thumb/Flash/USB Portable Storage Devices

Including portable storage devices that attach to the computer *via* a USB (Universal Serial Bus) connection or any other computer interface *device* or type

- b. Online Data Storage Services. Including services such as DropBox, Egnyte, OneDrive, Google Drive, and other solutions providing online data storage services;

## ACCEPTABLE USAGE OF IT RESOURCES

**POLICY NO. 103.001 (Eff. 09/07/2017)**

- c. **Wireless Connectivity**  
Including all computing devices utilizing radio frequency, microwave frequency, or infrared frequency communications methods and technologies;
- d. **Portable Computers**  
Including Laptop, Sub-notebook, Tablet, or Portable Personal Computing devices or systems;
- e. **Internet**  
Via commonly available browsers such as Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, and Opera;
- f. **Remote Terminal Access**  
Either *via* dial-up, LAN/WAN or wireless based access methods and terminal emulation and session emulation software applications;
- g. **E-mail**  
Including the State's Lotus Notes and/or Microsoft Outlook and Microsoft Office 365 e-mail systems, e-mail system, departmental e-mail and Internet e-mail accessed using State equipment;
- h. **Data Transfers and System Interfaces**  
Including all data transfers and systems interfaces to and from state computer systems and storage devices;
- i. **Personal Data Assistants (PDA's), cell phones, cell phone hybrids (e.g. smart phones), and all State owned and State authorized handheld access devices;**
- j. **Magnetic Media**  
Including flash/USB memory devices, disk, tape, cartridge, library, or disk/tape libraries or arrays;
- k. **Compact Disk (CD) and Digital Video Disk (DVD) media**  
Including all storage media utilizing laser encoding methods and techniques;
- l. **Hard Copy report output**  
Including all hardcopy report output, compilations, publications, assembled and unassembled reports, and

## ACCEPTABLE USAGE OF IT RESOURCES

**POLICY NO. 103.001 (Eff. 09/07/2017)**

other confidential paper based information generated by the State's computer systems;

- m. Weblogs (aka "BLOGS")  
Including all online weblogs (BLOGS), discussion boards, bulletin board systems, forums and FAQ columns;
- n. Instant Messaging/Chat  
Including Microsoft Instant Messaging and other online chat and messaging services;
- o. Streaming Audio or Video Online Services  
Including Netflix, Hulu, YouTube, Vimeo, Pandora, iHeart Radio, etc., for non-work related matters.

### D. Use for Profit and Solicitation

Users are strictly prohibited from using the State's IT resources for any personal or private financial gain, commercial or profit-making activities, and political, religious, or other solicitations.

### E. Unlawful and Unethical Conduct

- 1. Professional Communications:
  - a. Behave in a professional manner and shall exercise courtesy when using any electronic communication media;
  - b. Exercise the same degree of care, judgment, and responsibility in composing and transmitting electronic communications as would be done when composing and sending written communication;
  - c. Strictly refrain from the usage of profanity and/vulgarity when using any IT resource; and
  - d. Assume that an electronic message will be saved and reviewed by someone other than the intended recipients.
- 2. Discriminatory, Inappropriate and Offensive Communications

## ACCEPTABLE USAGE OF IT RESOURCES

**POLICY NO. 103.001 (Eff. 09/07/2017)**

- a. Users are strictly prohibited from using the State's IT resources to intentionally access, download from the Internet, display, transmit, or store any information that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, pornographic, violent, intimidating, libelous, defamatory, or is otherwise
- b. unlawful, inappropriate, and offensive, including but not limited to, offensive material concerning gambling, sex, race, color, national origin, religion, age, disability, or other characteristics that are protected by law;
- c. The Users' departmental policies such as the sexual harassment, workplace violence, and equal employment opportunity and affirmative action policies shall apply fully to the use of IT resources. Users are strictly prohibited from any actions that may violate such policies while using the State's IT resources; and
- d. Users are strictly prohibited from making defamatory comments or taking actions such as forwarding of electronic mail that facilitate the publication or spread of such comments.
- e. Users are strictly prohibited from sending, distributing or forwarding any and all e-mail via the State's electronic e-mail systems that the reasonable person would consider sexually explicit, profane, or offensive in any way, shape or form.

### 3. Attacking the System

Users shall not attempt, subvert, engage in, or contribute to any activity that would compromise the security of the State's IT resources. Activities that are expressly prohibited include, but are not limited to:

- a. Deliberately crashing, sabotaging, or damaging any computer system;
- b. Using software that is designed to destroy data, collect data, facilitate unauthorized access to information resources, or disrupt computing processes in any way; or

## ACCEPTABLE USAGE OF IT RESOURCES

POLICY NO. 103.001 (Eff. 09/07/2017)

c. Using invasive software that may cause viruses or other damage or expense.

### 4. Theft

Users are strictly prohibited from removing any hardware, software, attached peripherals, supplies, and documentation without the express approval of the department or agency head or designee.

Users are strictly prohibited from using diskettes, flash/USB memory devices, or other portable storage devices or storage media as defined in section C.2. in order to obtain restricted information.

### 5. Misrepresentation

Users are strictly prohibited from making unauthorized statements or commitments on behalf of the State or posting an unauthorized home page or similar web site.

## IX. DISCLAIMER OF LIABILITY FOR INTERNET USE

Users who access the Internet do so at their own risk. The State shall not be responsible for material viewed or downloaded by Users from the Internet.

Users are cautioned that pages might contain offensive, sexually explicit, and inappropriate material.

- X. This policy supersedes Department of Human Resources Development, Policy No. 103.001, Acceptable Usage of IT Resources, and effective May 25, 2004, as revised February 15, 2012.

## XI. AUTHORITIES AND REFERENCES

### A. AUTHORITIES

Chapter 26, Hawaii Revised Statutes, *Executive and Administrative Departments*

Chapter 84, Hawai'i Revised Statutes, *Standards of Conduct*

Chapter 92F, Hawaii Revised Statutes, *Uniform Information Practices Act*

**ACCEPTABLE USAGE OF IT RESOURCES**

**POLICY NO. 103.001 (Eff. 09/07/2017)**

Chapter 94, Hawaii Revised Statutes, *Public Archives; Disposal of Records*

**B. REFERENCES**

Department of Accounting and General Services *General Records Schedule 2002*, Revised through May 2006 Department of Human Resources Development, Director's Memorandum dated August 7, 2015, *Acceptable Usage of Information Technology Resources*

State Chief Information Officer's Memorandum OIMT-CORR 15.0105, dated August 11, 2015, *Blocking of Media Streaming Services on the State Network*

**XII. ATTACHMENTS**

Attachment A: Acceptable Usage of Information Technology Resources Acknowledgment Form, dated 9/7/2017