

# Enterprise Mobile Device Policy

DTS POLICY 5000-0003

---

**Status:** Active Policy

**Effective Date:** December 9, 2013

**Revised Date:** N/A

**Approved By:** Mark VanOrden, CIO

**Authority:** UCA 63F-1-103; Utah Administrative Code R895-7 Acceptable Use of Information Technology Resources; Utah Administrative Code, R477-11 Discipline

---

## Document History

**Originator:** Tim Hastings, Chief Information Security Officer

**Next Review:** January 2017

**Reviewed Date:** January 2016

**Reviewed By:** Philip Bates, Chief Information Security Officer

---

## 1.0 Purpose

### 1.01 Background

The following policy and guidelines inform State employees and contractors of their allowable usage and features with mobile computing devices available for business and limited personal use while connected to State networks and information technology assets.

This policy is necessary to protect the confidentiality, availability, and integrity of State of Utah secured information while stored, transmitted, or processed on mobile computing devices. Mobile devices are more susceptible to theft and loss in comparison to traditional desktop computing devices and additional security measures are needed. This policy is not applicable to State data and information that is available on State public Internet sites.

### 1.02 Definitions

- **Mobile device** - Any mobile computing device, mobile phone, tablet computer, or laptop computer that accesses and stores information.
- **State data** - Non-public information owned by the State of Utah that requires authentication (a user identification and password) for access.
- **Secure network** - The State's wired and wireless network used to access State data and resources including the UWDN network. Access to the Capnet network is not limited by this policy.
- **Mobile Device Management (MDM)** - A technology system that is used to ascertain if mobile devices attempting to connect to the network have required security controls configured.
- **Bring Your Own Device (BYOD)** - a concept that allows employees and contractors to utilize their personally-owned technology devices to stay connected to, access data from, or complete tasks for their organizations. At a minimum, BYOD programs allow users to access employer-provided services and/or data on their personal laptop computers, tablets, smartphones, and other devices.
- **Security protocols** - Configurations, settings and communication techniques on a device that control the confidentiality, integrity and availability of the devices data.
- **Operating System** - A collection of software that manages device hardware resources and provides common services for applications and computer programs.
- **Security Incident** - An event that compromises the confidentiality, integrity or availability of State data.

- **Encryption** - The process of encoding data in such a way that third parties cannot read it and only authorized parties can (currently iOS devices are encrypted by default and Android devices are not).
- **Firewall** - A software or hardware-based network security system that controls the incoming and outgoing network traffic by analyzing the data and determining whether they should be allowed through or not.
- **Supported Version** - A release of software and/or hardware that has been approved for State use and can be used to access and process State data

## 1.1 Scope

### 1.11

This policy applies to any mobile device that is used by the executive branch agencies to access and store State information or is used to access the secure network.

### 1.12

This policy applies to State employees and contractors accessing State data. Agencies should determine the best means of sharing data with outside parties including commissioners, board member and consultants. Communication methods and mediums should be considered before sharing information with them and security controls such as authentication and encryption should be considered for private and restricted data.

### 1.13

The policy establishes a baseline standard for all mobile devices, whether purchased by the State or personally purchased, and used by State employees for access to State data and networks. Agencies are required to adhere to these standards on all mobile devices and determine if additional security measures should be established for the needs of their individual data sets.

### 1.14

The Department of Technology Services (DTS) supports the Mobile Device Management (MDM) service to enforce the technology standards outlined in this policy. Agencies can administer these MDM services independently or can elect to have DTS perform this as a service for them. If Agencies choose to administer MDM services individually, DTS will annually assess the configurations for compliance with this policy.

## 2.0 Policy and Rules of Behavior

2.1 Any user with a mobile computing device accessing State data is subject to all DTS enterprise and agency policies, as well as federal, state and local statute governing acceptable use of State networks and information technology assets.

2.2 Smart phone and tablet devices (such as Android and iOS) will be configured to and users will agree to:

- Protect the State-owned and personal computing device from theft, damage, abuse, and unauthorized use.
- Notify the DTS Help Desk or Enterprise Information Security Office within one hour if the device is lost or stolen, or as soon as practical after they notice the device is missing.
- Follow the Enterprise Information Security Policy 5000-0002, Section 2.3.1 Media Protection when connecting external devices to mobile devices for data storage (using encrypted disks to store any sensitive information).

- Connect to State networks using the security protocols required by your Agency. This may include use of secured network connections and use of State approved Virtual Private Network (VPN) services.
- Receive and install security and other operating system updates from the operating system vendor.
- Install Mobile Device Management software and applications on their device prior to connecting them to State systems.
- Use a 4-digit device password or thumb print reader on smart phones and tablets.
- Agree that DTS may restrict the access of any mobile computing device to State networks if the mobile computing device presents a probable and demonstrable threat to the integrity of State data or other computing resources.
- Encrypt the data on their device where State data is stored.
- Agencies may determine that personally owned mobile computing devices can connect to the State network and be used for business purposes. [Personal devices that are used to access and store State data must meet the following requirements:](#)
  - Allow the State access, for discovery purposes, to the content stored on the device when it is believed to be connected to a security incident;
  - Give the State the right to remotely disable or wipe the State data stored on the mobile device in the event the device is lost or stolen;
  - Install a Mobile Device Management agent requiring device encryption, a 4-digit passcode (or thumb print reader) and anti-virus (antivirus on Android devices only).

### 2.3 Laptop computers will be configured to and users will agree to:

- Protect the State-owned and personal computing device from theft, damage, abuse, and unauthorized use.
- Notify the DTS Help Desk or Enterprise Information Security Office within one hour if the device is lost or stolen, or as soon as practical after they notice the device is missing.
- Not use personally owned data storage devices and media (USB Flash Drives, CD/DVD, Portable Hard Drives, etc.,) to capture and store State-owned information assets.
- Connect to State networks using the security protocols required by your Agency. This may include use of secured network connections and use of State approved Virtual Private Network (VPN) services.
- Receive and install security and other operating system updates from the operating system vendor.
- Use a password compliant with the 4000-0002 Enterprise Password Standards Policy.
- Agree that DTS may restrict the access of any laptop to State networks if the device presents a probable and demonstrable threat to the integrity of State data or other computing resources.
- Encrypt the data on their laptop if connected to the State network.
- Agencies may determine that personally owned laptops can connect to the State network and be used for business purposes. Personal laptops that are used to access and store State data must meet the following requirements:
  - Allow the State access, for discovery purposes, to the content stored on the device when it is believed to be connected to a security incident;
  - Give the State the right to remotely disable or wipe the content of the device in the event the device is lost or stolen;
  - Install anti-virus software that actively scans for security threats and receives regular updates of new viruses;

- Install and activate encryption of all State data stored on the laptop or activate whole-disk encryption (Filevault for Apple computers and Bitlocker for Windows computers);
- And activate the laptop's firewall to block incoming traffic to the device.

2.4 Access to and continued use of network services is granted on the condition that each employee or contractor reads, signs, respects, and follows Enterprise and Agency policies concerning the use of computing devices while connected to State-owned networks and/or information assets.

2.5 Personally owned devices used for State business purposes agree to the following:

- DTS does not provide technical support for personally owned devices,
- Users acknowledge that when State data is stored on personally owned devices, the contents of these devices could be subject to GRAMA requests, and
- Users agree to hold the State harmless for any damage to the device or its operating system and related software as a consequence of using the State network or other computing resources.

2.6 Current Mobile Devices Approved for State use:

Android Smart Phones & Tablets version 4.X or higher

iOS iPhones & iPads

Windows Based Laptop Computers (only DTS supported versions)

Mac OSX Based Laptops

Google Chrome OS

This list of approved devices will be maintained in the Desktop Services product description at the following link:

<http://dts.utah.gov/get-a-product-service/desktop-services.php>

2.7 Personal data storage devices (USB Flash Drives, CD/DVD, Portable Hard Drives, etc.) are not approved for use. State information should not be stored on personally owned mobile devices outside of native email, calendar, and State approved applications.

2.8 Expectation of Privacy

State of Utah employees and contractors do not have a right, nor should they have an expectation, of privacy while using State-owned personal computing and data storage devices connected to or using State-owned networks and information technology assets, including accessing the Internet and using e-mail and voice communications. The Department of Technology Services will respect the privacy of employee and contractor personal devices and will only request access to the device by technicians to implement security controls, as outlined by enterprise policy directives, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings. This differs from policy for State-owned or provided equipment/services, where State employees and contractors do not have the right, nor should they have the expectation, of privacy while using State-owned equipment or services. If questions arise related to compliance with these security requirements, State employees and contractors may opt to drop out of the BYOD program versus providing the device to technicians for compliance verification. Should a user opt out of the BYOD program, it is expected the personal device is not used to access State resources.

### **3.0 Policy Compliance**

State of Utah employees and contractors are expected to comply with this policy. Additional policies and standards developed and implemented by State Agencies may include additional objectives or detail, but must be compatible with the security objectives described in this policy document.

### **4.0 Enforcement**

Violation of this policy by personnel employed by the State of Utah may be the basis for discipline including but not limited to termination. Individuals and contractors working with any State of Utah Agency found to have violated this policy may also be subject to legal penalties as may be prescribed by state and/or federal statute, rule, and/or regulation.

**UTAH DEPARTMENT OF HUMAN SERVICES  
POLICY AND PROCEDURES**

**Reference: 06-02**

**Effective Date: November 8, 1994  
Revision Date: March 1, 2013**

**Page 1 of 3**

**SUBJECT: CELL PHONES AND LAND-LINE TELEPHONES**

**RATIONALE: The Department of Human Services (DHS) requires cost effective options in meeting cell phone and land-line telephone needs and effectively serving clients; securing State data and information while it is stored, transmitted, or processed on a cell phone; and justification of business need for an employee’s use of a cell phone for State business.**

**I. Definitions**

- A. Business need – A need which supports a business goal or objective of a DHS work unit. Examples of business needs include: (1) the work unit’s need to contact the employee for work-related issues, (2) the work unit’s need that the employee be available to speak with clients in the field, and (3) the employee’s need to speak with clients outside the employee’s normal work day. Ineligible business needs include (these do not meet the criteria for providing an employee a cell phone because they create a taxable situation under the IRS guidelines): (1) to promote the morale or good will of an employee, (2) to attract a prospective employee, or (3) to provide additional employee compensation.
- B. Cell phone –any device that is designed to be moved, excluding laptops, and is capable of collecting, storing, transmitting, or processing electronic data or images. Examples include a tablet (e.g iPad), iPhone, Blackberry, Smartphone, or mobile network connected storage device.

**II. Policy**

- A. Business Need for a Cell Phone. The agency must justify an employee’s business need for a cell phone. If the business need cannot be clearly identified, no State cell phone or reimbursement (ongoing) shall be provided. Business need must be documented, signed by the appropriate individuals, retained indefinitely, or for one year after the last reimbursement, and evaluated annually using **Form A** or **Form B**.
- B. Personal Use of a State Cell Phone. Personal use of a State cell phone must be de minimis (short and infrequent) and is generally limited to incidental and occasional use in accordance with *DHS policy and procedure 06-04 on “Appropriate Use of Information Technology Resources”* and *Administrative Rule 895-7 on “Acceptable Use of Information Technology Resources.”*
- C. Reimbursement for Business Use of a Personal Cell Phone. There are two options in which an employee may be reimbursed for using a personal cell phone for State business:

- 1. Per-pay-period reimbursement (ongoing) for cell phone services:

Voice	\$14	Text	\$2	Navigation	\$5	International	\$2
Data	\$10	Tethering (wi-fi)	\$4	Emergency Priority	\$2		

**\*\*\*IMPORTANT\*\*\* *The employee’s share of the personal phone bill cannot be less than the reimbursement amount, and the calculation must be approved by the work unit manager. (See Form B for further detail.) DHS work units may set their own cell phone reimbursement rates as long as they are more restrictive (less costly to the State) than these reimbursement rates, and they should be included in the work unit’s policy.***

- 2. Occasional reimbursement of voice service at five cents per minute. Occasional reimbursement requires management approval on the Employee Reimbursement/Earnings Request, Form FI 48, with the copy of the original bill attached. (See *FIACCT 05-05.00, Procedures, Occasional Reimb. of Actual Telecommunications Expenses - nontaxable.*)
- D. Security. Any cell phone, whether State or personal, that stores or transmits State data or information must be in compliance with *Department of Technology Services (DTS) policy on*

**UTAH DEPARTMENT OF HUMAN SERVICES  
POLICY AND PROCEDURES**

**Reference: 06-02**

**Effective Date: November 8, 1994  
Revision Date: March 1, 2013**

**Page 2 of 3**

**SUBJECT: CELL PHONES AND LAND-LINE TELEPHONES**

*“Using Network Capable Mobile Computing Devices to Store or Access Secured State Information”* and, in addition, must have:

1. Encryption enabled on the cell phone.
  2. State-required software kept up to date (e.g. anti-virus, etc.).
  3. Only approved third-party applications installed in the State’s container on the cell phone.
  4. State data or information on the cell phone backed up using DTS approved services each time the cell phone connects to State networks.
- E. Prohibited and Discouraged Use of a Cell Phone. Use of a cell phone to make or receive telephone calls while operating a motor vehicle is discouraged, and it is illegal to:
1. text message;
  2. manually communicate through an electronic mail system;
  3. manually enter data into a handheld wireless communication device;
  4. send data, read text, or view images on a handheld wireless communication device; or
  5. manipulate an application from a handheld wireless communication device.
- (See *Utah Code 41-6a-1716*.)
- F. This policy supplements other administrative rules and policies established by the State. Employees are required to be knowledgeable of and comply with these rules and policies, including:
1. DHS policies and procedures 02-03 on “Code of Ethics;” (in particular section II.B) and 06-04 on “Appropriate Use of Information Technology Resources” (in particular sections 4.a, 4.b, 4.c, and 5.);
  2. DTS Administrative Rule 895-7 on “Acceptable Use of Information Technology Resources” and policy 4300-0030 on “Using Network Capable Mobile Computing Devices to Store or Access Secured State Information;” and
  3. State Division of Finance accounting policy and procedure FIACCT 05-05.00 on “Cell Phones and Home Internet Service – State-provided, Employee Allowances or Reimbursements.”
- G. Privacy of Data on Personal Equipment. Privacy of data on personal cell phones is subject to *FIACCT 05-05, Policy, J*. Personal data may be viewed by a State officer or court.
- H. More Than One Phone Per Employee. Management should evaluate whether employees need two phones (land-line and cell phone) to meet their business need. Where two phones are not needed, management should consider eliminating one.
- I. Personal long-distance calls made on a State land-line telephone must be reimbursed to the work unit at five cents per minute.

**III Responsibilities**

A. Division’s Main Budget Office Responsibilities

1. Designate work unit manager(s).
2. Maintain list of designated work unit manager(s).

B. Work Unit Manager Responsibilities.

1. Designate cell phone coordinator(s) to assist work unit manager.
2. Approve **Forms A and B**. Develop monitoring procedures and monitor:
  - a. State cell phone usage to ensure personal use is within the guidelines in the *DHS policy and procedure 06-04 on Appropriate Use of Information Technology Resources*. Monitoring of personal use should occur on a monthly basis and should focus on

**UTAH DEPARTMENT OF HUMAN SERVICES  
POLICY AND PROCEDURES**

**Reference: 06-02**

**Effective Date: November 8, 1994**

**Page 3 of 3**

**Revision Date: March 1, 2013**

**SUBJECT: CELL PHONES AND LAND-LINE TELEPHONES**

employees with high minute use, large number of texts, and/or a large amount of data usage, and ensure personal use is within the guidelines in the policy. (Can be verbal discussion; does not require highlighting personal use on the cell phone bill.) This monitoring should be documented and available for audits.

- b. Personal cell phone reimbursements (ongoing) to ensure cell phone services are still needed for State business. Monitoring of services needed for State business should occur on an annual basis and should ensure the reimbursements do not include extra services that are not justified by business need.
  3. Consider the option of allowing employees to share a State-provided cell phone when circumstances do not justify acquisition of a cell phone for an employee's exclusive use. All State-provided cell phones intended to be shared among work unit employees shall be registered in the name of the cell phone coordinator.
  4. When an employee terminates or transfers positions, notify the DTS Help Desk at (801) 538-5772 to remove all State information and data on the employee's personal cell phone.
  5. Initially and annually by May 30, require each employee who has been authorized to use a cell phone to complete a new **Form A** or **Form B** to ensure the State business need still applies. Keep these completed and signed agreements in the work unit files. At least annually, the work unit manager shall review the cost efficiency and performance of his/her Division, Office, Region, Bureau, or Institution cell phone carrier plan.
  6. Submit a copy of **Form B** to the Division's Main Budget Office for review. The Division's Main Budget Office will request State Payroll to set up a recurring payroll payment using the nontaxable Wage Type 1182 (Telephone Reimbursement). (See *FIACCT 05-05.00 Procedures, Employee-Provided Cell Phone - Nontaxable Allowance, paragraph 8.*)
- C. Cell phone Coordinator Responsibilities
1. Ensure that:
    - a. All required forms are completed accurately, including all required signatures;
    - b. A copy of the employee's personal cell phone bill used to determine the reimbursement is attached; and
    - c. All forms and personal cell phone bills are retained in a work unit file.
  2. Prepare and maintain a work unit list of all approved State cell phone and personal cell phone users. The list shall include, at a minimum, the approved user's name, work location, cell phone number, brand, model, serial number or other identification number, and carrier. When a State-provided cell phone is reassigned to another employee for State business use, update the list of approved State-provided cell phone users to reflect the reassignment.
  3. Maintain a checkout system for all State-provided cell phones available for use by more than one employee. Each time an employee uses a shared State-provided cell phone, the employee shall sign **Form C** in addition to completing **Form A**.

IV. Attachments

Form A – State Cell Phone Agreement

Form B – Personal Cell Phone Reimbursement Agreement

Form C – Shared State Cell Phone Checkout Sheet



Palmer DePaulis, Executive Director  
Department of Human Services

DATE: March 1, 2013

<b>UTAH DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES</b>		
<b>Reference: 06-04</b>	<b>Effective Date: October 20, 1997 Revision Date: June 3, 2013</b>	<b>Page 1 of 10</b>
<b>SUBJECT: POLICY ON THE APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES</b>		
<b>RATIONALE: The purpose of this policy is to ensure that information technology resources ("IT Resources") owned or operated by the State of Utah or the Utah Department of Human Services are used efficiently and appropriately. This policy is also designed to notify Department employees and others about how they may (and may not) use IT Resources, and about how the Department will monitor and enforce this policy.</b>		

1. **Department's Policy Regarding the Appropriate Use of IT Resources:** It is the policy of the Utah Department of Human Services (the "Department") that IT Resources are valuable government resources that must be used efficiently and appropriately to carry out the business of the State of Utah (the "State") and the Department. The Department will monitor and enforce this policy to ensure that its employees and other users do not use IT Resources for impermissible personal uses or for any other uses that violate this policy.
  
2. **Scope of This Policy:** This policy supplements any statutes, rules and policies established by the State, including: (a) Rule 365-7 on "information technology protection"; and (b) "acceptable use" policies adopted by the State's Chief Information Officer pursuant to Utah Code Ann. § 63D-1a-301.
  
3. **Definitions Used in This Policy:**
  - a. **"IT Resources"** means a wide range of information technology resources owned or operated by the State or the Department, including:
    - (1) Computer hardware. The physical components of a computer system and related devices. Examples of hardware include motherboards, disk drives, memory, monitors, keyboards, mice, printers, and scanners;
    - (2) Computer software. A set of instructions that cause a computer to perform one or more tasks. Computer software comprises the entire set of programs, procedures, and routines associated with the operation of a computer system. Three main types of software are system software, application software, and information systems:
      - a. System software. Programs and processing routines that control a computer's internal functioning, chiefly through an operating system, and also controls such peripherals as monitors, printers, mice and storage devices. Examples of system software include operating systems (Windows, Linux, UNIX, NetWare) and utility programs (sort, merge, backup);
      - b. Application software. Programs designed to handle specialized tasks; many of which are sold or licensed as ready-to-use packages. Examples of application software include general-purpose spreadsheet and word

<b>UTAH DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES</b>		
<b>Reference: 06-04</b>	<b>Effective Date: October 20, 1997 Revision Date: June 3, 2013</b>	<b>Page 2 of 10</b>
<b>SUBJECT: POLICY ON THE APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES</b>		

processing programs, Internet browsers, programming languages (Basic, C++, Java, PowerBuilder); and

c. Information systems. An integrated set of programs and organized procedures for collecting, storing, processing, communicating information, decision making, and control in the organization. Information systems are tailored to meet the unique business requirements of the organization. Examples of information systems include CARE, Data Warehouse, Echart, FINET, HRE, ORSIS, Payroll, SAFE, SAMHIS, USSDS, and USTEPS;

- (3) Electronic mail ("e-mail");
- (4) Electronic voice and video communications (including voice mail);
- (5) Information storage media (including hard disks, floppy disks, zip disks and the electronic files and records contained on those disks);
- (6) Telecommunications equipment;
- (7) Facsimile equipment and facsimiles (often called faxes);
- (8) The Internet;
- (9) Logs or similar records that indicate Internet use or access, and information downloaded from the Internet; and
- (10) Future technologies owned, provided or operated by the State or the Department.

**NOTE:** All items listed in the definition of "IT Resources" are the property of the State and the Department. Under state and federal law, files and other contents of these IT Resources may be regarded as "records" of the State or the Department. For example, depending on its content, an e-mail message may be a "record" under GRAMA (Utah's Government Records Access and Management Act).

- b. **"User"** of IT Resources means all Department employees, volunteers, contract providers and others who have accessed or who currently have access to IT Resources.
- c. **"Use"** means any use of IT Resources. The term "use" shall be broadly interpreted to include such activities as preparing, sending, accessing, viewing, retrieving, downloading, faxing, copying and printing documents, files and programs, or using telecommunication resources such as phones and faxes.

<b>UTAH DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES</b>		
<b>Reference: 06-04</b>	<b>Effective Date: October 20, 1997</b>	<b>Page 3 of 10</b>
	<b>Revision Date: June 3, 2013</b>	
<b>SUBJECT: POLICY ON THE APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES</b>		

- d. **"Computer Virus"** means any program that can destroy application software or data files, or which can disrupt the operation of IT Resources. (IT Resources can be contaminated by viruses in many ways, including downloading files from the Internet, using pirated (unlicensed) software, and opening email attachments that contain viruses.)
  
- e. **"Personal Use"** means any use of IT Resources that is not reasonably relevant or applicable to the User's job-related duties for the Department. "Personal Use" includes such activities as correspondence (electronic or otherwise), games, transactions (including sales and purchases), calculations, downloading or accessing information, and other commercial, social, charitable, religious, political or recreational activities that are not related to the User's job.
  
- f. **"Monitor"** means to access, observe, review, audit, intercept and disclose a User's use of IT Resources. Monitoring may be random or may be focused on a specific User.

**4. Uses of IT Resources.**

- a. **Unauthorized Uses of IT Resources:** The following uses of IT Resources are always prohibited:
  - (1) **Illegal, Disruptive, Inefficient, Destructive or Risky Uses:** Users may not use IT Resources to engage in any activity that:
    - a. violates federal, state or local statutes, regulations or policies;
    - b. disrupts or distracts from the conduct of State or Department business;
    - c. reduces job productivity, or unreasonably expends the resources of the State or the Department;
    - d. alters, destroys, dismantles or disfigures IT Resources;
    - e. creates a security risk to IT Resources, or disrupts the use or performance of IT Resources; or
    - f. involves the storage of unauthorized data or software on IT Resources;
  
  - (2) **Private Business Uses:** A User may not use IT Resources to run a private business or engage in conduct related to the User's personal enterprises or commercial activities, including the preparation or transmittal of any correspondence, records, billings, advertisements or solicitations related to such activities;
  
  - (3) **Religious or Political Uses:** A User may not use IT Resources to prepare or send any religious or political communications, including correspondence, petitions, brochures, tracts, position statements or announcements, if those

<b>UTAH DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES</b>		
<b>Reference: 06-04</b>	<b>Effective Date: October 20, 1997</b>	<b>Page 4 of 10</b>
	<b>Revision Date: June 3, 2013</b>	
<b>SUBJECT: POLICY ON THE APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES</b>		

communications involve proselytizing, solicitation, lobbying, advertising, fund-raising or more than minimal use of the Department's resources;

- (4) **Sexually Explicit or Pornographic Uses:** A User may not use IT Resources to access, review, send, retrieve or print any sexually explicit or pornographic material (regardless of whether it is pictorial or textual, and regardless of whether it is technically "obscene" under state and federal laws) unless the material is reasonably relevant to and necessary for the performance of the User's job-related duties. The User shall have the burden of proving that any such use was reasonably relevant to and necessary for the performance of the User's job-related duties, unless the User obtains prior written approval from the User's supervisor, authorizing such access or use of sexually explicit or pornographic material, and unless the supervisor files a copy of such approval in the User's personnel file or contract file;
- (5) **Illegal Copying or Pirating:** A User may not use IT Resources to copy, send, "pirate" or use software, copyrighted materials or another person's original writings or programs, in violation of copyright license agreements or laws;
- (6) **Inappropriate Access to Confidential or Restricted Material:** A User may not use IT Resources to access information which is classified or treated as confidential or otherwise restricted, unless the User is authorized to access such information under applicable laws, statutes, regulations or policies;
- (7) **"Hacking" and Other Forms of Unauthorized Access:** A User may not use IT Resources to access or "hack" into unauthorized files, programs, applications or other IT Resources, or to obtain access to any IT Resources to which the User has no job-related need or for which the User is not authorized to access;
- (8) **Masquerading As Another User:** A User may not use IT Resources to masquerade as another User, or to read, examine, disclose, copy or alter the personal files of another User, unless such activities are: (a) authorized by the User; or (b) approved by the User's supervisor and permitted by state or federal law or this policy;
- (9) **Harassment:** A User may not use IT Resources to send information that may reasonably be interpreted as harassment of others based on race, national origin, sex, sexual orientation, age, disability, religion, or political affiliation;
- (10) **Spreading Computer Viruses:** A User may not use IT Resources to knowingly or negligently spread a computer virus;

<b>UTAH DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES</b>		
<b>Reference: 06-04</b>	<b>Effective Date: October 20, 1997</b>	<b>Page 5 of 10</b>
	<b>Revision Date: June 3, 2013</b>	
<b>SUBJECT: POLICY ON THE APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES</b>		

- (11) **Junk Mail:** A User may not use IT Resources to distribute "junk" mail such as chain letters, advertisements or solicitations;
- (12) **Inappropriate Use of Printers:** A User may not use a Department printer for personal use or for large print jobs which could be done less expensively and more efficiently by using available photocopiers or offset presses; or
- (13) **Careless Use of Confidential Information:** A User may not use IT Resources to send confidential or otherwise-restricted information without taking proper precautions (such as encryption) to ensure that the transmission is secure. (The Governmental Records Access and Management Act ("GRAMA") and many other state and federal laws restrict public access to certain records, including electronic records, maintained by the Department.)

b. **Penalties for the Unauthorized Use of IT Resources:** The unauthorized use of IT Resources may result in one or more of the following: removal of privileges to IT Resources; corrective action or disciplinary action (including termination) in accordance with the State's Human Resource Management Rules; civil action; and criminal prosecution under state or federal laws and regulations regarding the use of IT Resources. See, e.g., The Electronic Communications Privacy Act of 1986 (18 U.S.C. § 1367 et. seq.), the Computer Fraud and Abuse Act of 1986 (18 U.S.C. § 1030 et. seq.), the Utah Computer Crimes Act (Utah Code Ann. § 76-6-701 et. seq.), rules regarding "Information Technology Protection" (Utah Admin. Code R895-7-4 et. seq.), and rules of the Utah Department of Human Resource Management, Utah Admin. Code 477-9-6.

- (1) **"Zero Tolerance" for Pornography and Sexually Explicit Materials:** The Department has "zero tolerance" for using IT Resources to access or transmit pornographic materials in violation of this policy, and such uses will result in termination of the User's employment or contract with the Department. Using IT Resources to access or transmit sexually explicit materials may also result in termination, depending on the nature of the material.

c. **Personal Use of IT Resources:** IT Resources may be used only in conjunction with a User's job-related duties, except as provided in this section. Frequent or extensive non-job-related use of IT Resources reduces job productivity, and is not permissible. However, certain incidental and occasional Personal Use of IT Resources is permitted during lunch or break periods or for short periods of time before or after regular working hours, as long as such use does not:

- (1) Involve an Unauthorized Use of IT Resources (see Section (4)(a) above);
- (2) Have the potential to embarrass the State or the Department;

<b>UTAH DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES</b>		
<b>Reference: 06-04</b>	<b>Effective Date: October 20, 1997</b>	<b>Page 6 of 10</b>
	<b>Revision Date: June 3, 2013</b>	
<b>SUBJECT: POLICY ON THE APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES</b>		

- (3) Involve generalized or widespread publication or disclosure of a Department-based (or State-based) e-mail address or similar identifying information, such as can occur when a User sends jokes to a large number of friends by e-mail, or when a User accesses an electronic chat room, an electronic bulletin board or an electronic auction service;
- (4) Involve sending or receiving frequent or numerous non-job-related messages (such as e-mails, faxes or advertisements);
- (5) Incur a cost that the User must reimburse to the State or the Department, unless the Department has authorized such use and reimbursements in advance; or
- (6) Involve the storage of more than 20 megabytes (MB) of data on the Department's hard drives or network.

**Examples of Permissible and Non-Permissible Personal Uses:**

- A User may make an occasional purchase from an on-line catalog such as Lands' End during the User's break times, as long as the merchandise is delivered to the User's home, and as long as the User does not authorize Lands' End to send advertisements or other materials to the User's e-mail address at the Department.
- Even during lunch or break times, however, a User may not use IT Resources to participate in a recreational chat room or an electronic auction such as e-Bay.
- A User may never access pornographic material or order anything from an on-line source that offers sexually explicit material, unless a supervisor gives prior written approval in accordance with Section (4)(a)(4) above.
- A User may use IT Resources during the User's break times to type up a small calendar events for the User's church group, but a User may not use IT Resources to prepare a proselytizing brochure or a fund-raising letter for the church group.
- A User may not use IT Resources to receive regular or automated investment information or announcements about airline ticket prices.

<b>UTAH DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES</b>		
<b>Reference: 06-04</b>	<b>Effective Date: October 20, 1997</b>	<b>Page 7 of 10</b>
	<b>Revision Date: June 3, 2013</b>	
<b>SUBJECT: POLICY ON THE APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES</b>		

**NOTE:** This list of examples is intended to help Users understand the policy on IT Resources. It is not intended as an exhaustive list of permissible and non-permissible Personal Uses.

- 5. Mobile Computing Devices:** The use of mobile computing devices such as laptops, cell phones, smart phones, digital recording devices, thumb drives, or any device capable of storing data must be protected from being lost or stolen. The following list will be helpful in preventing such loss.
- a. Mobile computing devices that contain Personal Identifiable Information (PII) or sensitive information from state systems should be password protected and encrypted so stored information won't be compromised if the device is lost or stolen.
  - b. Only approved State owned mobile devices that are password protected and encrypted should be used for storing for state data. (DTS will assist in obtaining the appropriate devices).
  - c. Mobile computing devices that contain PII or sensitive information should be physically secured at all times:
    - (1) Never leave a mobile computing device in an unattended vehicle where it can be seen. Such devices should be locked in the trunk.
    - (2) Never leave a mobile computing device overnight in an unattended vehicle.
    - (3) Hand-carry or keep mobile computing devices under visual observation while traveling on public transportation.
    - (4) Use a cable lock to anchor laptops to a fixed object in the room during hotel stays.
    - (5) Do not leave a mobile computing device in an unattended, unsecured personal residence.
    - (6) Do not leave a mobile computing device unattended and unsecured in the workplace. Unless in a locked office, mobile computing devices should be locked in a container or secured with a cable lock to an immovable object.
  - d. If a mobile computing device is lost or stolen the incident must be reported to the supervisor and the Office/Division Director within one business day of becoming aware of the incident.

<b>UTAH DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES</b>		
<b>Reference: 06-04</b>	<b>Effective Date: October 20, 1997</b>	<b>Page 8 of 10</b>
	<b>Revision Date: June 3, 2013</b>	
<b>SUBJECT: POLICY ON THE APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES</b>		

6. **Monitoring of IT Resources:** The Department has the right, at its discretion, to monitor its IT Resources to ensure that they are being used appropriately and are functioning properly. See, e.g., Utah Admin. Code R895-7-4 et seq. This means that the Department may monitor a User's individual use of IT Resources (including e-mail messages and other documents) for any reason without notifying the User in advance. Although this policy allows Users to engage in certain Personal Uses of IT Resources, Users do not have any expectation that they can use such IT Resources free of the Department's monitoring or scrutiny.
7. **Reporting of Unauthorized Use of IT Resources:** Any User who receives a complaint or otherwise becomes aware of an Unauthorized Use of IT Resources shall report this information to the appropriate Human Resource Specialist in the Department's Office of Human Resources. The Human Resource Specialist will work as needed with representatives of management, the Department Technology Services and the Bureau of Internal Audit and Review to investigate the nature and extent of the alleged Inappropriate Use, and shall submit findings to management.
8. **Appropriate Choice of IT Resources:** Users must exercise good judgment about when and how they use IT Resources. For example, sending an e-mail message creates a written record of your communication, and e-mails are easily forwarded (inadvertently or intentionally) to recipients other than the ones you intended. This can lead to awkward situations for you and the Department. Similarly, firing off an indiscreet or angry e-mail message can create a whole host of difficult problems for you and the Department. Users also need to remember that various federal and state laws (such as GRAMA) may require agencies and individuals to disclose certain records, including electronic records such as e-mail, faxes, word processing documents, pagers, and the Internet. Moreover, in some cases, the Department may be required to disclose e-mail messages or computer documents to the opposing party in a lawsuit. With this in mind, Users of IT Resources should be aware of the value and sensitivity of information produced by their IT activities, and they should give adequate consideration to selecting an appropriate method of using, storing or delivering each message or information.
9. **Additional Software:** Users may install and maintain additional commercial software (i.e., software that is not provided by the State or the Department) on their workstations only if:
- a. Installing or using the software complies with all licensing and copyright laws, and the User has retained documentation showing that the User owns or is licensed to use the software;
  - b. The software supports a job-related function;

<b>UTAH DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES</b>		
<b>Reference: 06-04</b>	<b>Effective Date: October 20, 1997</b> <b>Revision Date: June 3, 2013</b>	<b>Page 9 of 10</b>
<b>SUBJECT: POLICY ON THE APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES</b>		

- c. The User has obtained the Department's or Division's approval before installing the commercial software; and
- d. The User's supervisor files a copy of this approval in the User's personnel or contract file.

**10. Procedures for Accessing IT Resources:**

**a. DHS Network Access Request Form:**

- (1) All Users of IT Resources shall sign the DHS Network Access Request Form, certifying that they have read and will comply with the DHS Policy on the Appropriate Use of Information Technology Resources. The DHS Network Access Request Form shall contain the following statement:

**I have read, understand and agree to comply with the Department's "Policy on the Appropriate Use of Information Technology Resources." I have discussed any questions and issues of concern with my supervisor or contract manager in the Department, and these matters have been resolved to my satisfaction.**

**User's Signature: \_\_\_\_\_ Date: \_\_\_\_\_**

- (2) A new User may not obtain access to IT Resources until that User and his/her supervisor have signed the DHS Network Access Request Form.
  - (3) The Department may periodically require Users and their supervisors to complete the DHS Network Access Request Form re-certifying that they understand and will comply with the DHS Policy on the Appropriate Use of Information Technology Resources.
  - (4) The User's supervisor shall maintain the completed DHS Network Access Request Forms in the User's Human Resources (HR) file or contract file.
- b. User Accounts:** The Department of Technology Services (DTS), Security Group or Help Desk shall not establish a User account for any person who requires access to an information system until that user and his/her supervisor have signed the appropriate authorization form for that information system. The User's supervisor shall evaluate the User's job responsibilities and determine the appropriate level of access to the information system, based on a "need to know/need to do" factors. The supervisor shall submit the completed authorization form to DTS, the Security Group or Help Desk

<b>UTAH DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES</b>		
<b>Reference: 06-04</b>	<b>Effective Date: October 20, 1997</b>	<b>Page 10 of 10</b>
	<b>Revision Date: June 3, 2013</b>	
<b>SUBJECT: POLICY ON THE APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES</b>		

- c. indicating the level of access required to carry out the User's job. DTS, the Security Group or Help Desk responsible for creating a User account shall maintain the completed access request form in their office.
  
- d. **Password and Access Security:**
  - (1) Users are responsible for maintaining the security of their passwords. Users may not share, post or display their logon id's or passwords.
  - (2) Passwords shall be at least six characters long.
  - (3) Passwords shall be changed at least once every ninety (90) days, or more frequently if the User requests.
  - (4) Users shall change their passwords whenever a security problem is identified by the User or the Division or the Department of Technology Services.
  - (5) Each account shall have six (6) grace logons before the account is locked. The Department of Technology Services will unlock a User's account only if a satisfactory response is received from the User about the failed attempts.
  
- d. **Security Procedures When a User Transfers or Leaves the Department:** The User's supervisor or contract manager shall collect all IT Resources assigned to the User and shall ensure that access to IT Resources is terminated. The supervisor or contract manager shall notify DTS, the Security Group or Help Desk to close the user's account.

An "exit interview form" may be used for this purpose, and can be obtained from the following on-line site: <http://www.hsemployees.utah.gov/ot/forms/exitinte.pdf>.

Palmer DePaulis DATE 6/5/2013  
Palmer DePaulis, Executive Director  
Department of Human Services

**R895. Technology Services, Administration.**

**R895-7. Acceptable Use of Information Technology Resources.**

**R895-7-1. Purpose.**

Information technology resources are provided to state employees to assist in the efficient day to day operations of state agencies.

Employees shall use information technology resources in compliance with this rule.

**R895-7-2. Application.**

All agencies of the executive branch of state government including its administrative sub-units, except the State Board of Education and the Board of Regents and institutions of higher education, shall comply with this rule.

**R895-7-3. Authority.**

This rule is issued by the Chief Information Officer under the authority of Section 63F-1-206 of the Utah Technology Governance Act, Utah Code, and in accordance with Section 63G-3-201 of the Utah Rulemaking Act, Utah Code.

**R895-7-4. Employee and Management Conduct.**

(1) Providing IT resources to an employee does not imply an expectation of privacy. Agency management may:

(a) View, authorize access to, and disclose the contents of electronic files or communications, as required for legal, audit, or legitimate state operational or management purposes;

(b) Monitor the network or email system including the content of electronic messages, including stored files, documents, or communications as are displayed in real-time by employees, when required for state business and within the officially authorized scope of the person's employment.

(2) An employee may engage in incidental and occasional personal use of IT resources provided that such use does not:

(a) Disrupt or distract the conduct of state business due to volume, timing, or frequency;

(b) Involve solicitation;

(c) Involve for-profit personal business activity;

(d) Involve actions, which are intended to harm or otherwise disadvantage the state; or

(e) Involve illegal and/or activities prohibited by this rule.

(3) An employee shall:

(a) comply with the Government Records Access and Management Act, as found in Section 63G-2-101 et seq., Utah Code, when transmitting information with state provided IT resources.

(b) Report to agency management any computer security breaches, or the receipt of unauthorized or unintended information.

(4) While using state provided IT resources, an employee may not:

(a) Access private, protected or controlled records regardless of the electronic form without data owner authorization;

(b) Divulge or make known his/her own password(s) to another person;

(c) Distribute offensive, disparaging or harassing statements including those that might incite violence or that are based on race,

national origin, sex, sexual orientation, age, disability or political or religious beliefs;

(d) Distribute information that describes or promotes the illegal use of weapons or devices including those associated with terrorist activities;

(e) View, transmit, retrieve, save, print or solicit sexually-oriented messages or images;

(f) Use state-provided IT resources to violate any local, state, or federal law;

(g) Use state-provided IT resources for commercial purposes, product advertisements or "for-profit" personal activity;

(h) Use state-provided IT resources for religious or political functions, including lobbying as defined according to Section 36-11-102, Utah Code, and rule R623-1;

(i) Represent oneself as someone else including either a fictional or real person;

(j) Knowingly or recklessly spread computer viruses, including acting in a way that effectively opens file types known to spread computer viruses particularly from unknown sources or from sources from which the file would not be reasonably expected to be connected with;

(k) Create and distribute or redistribute "junk" electronic communications, such as chain letters, advertisements, or unauthorized solicitations;

(l) Knowingly compromise the confidentiality, integrity or availability of the State's information resources.

(5) Once agency management determines that an employee has violated this rule, they may impose disciplinary actions in accordance with the provisions of DHRM rule R477-11-1.

**KEY: information technology resources, acceptable use**

**Date of Enactment or Last Substantive Amendment: September 11, 2014**

**Notice of Continuation: April 15, 2014**

**Authorizing, and Implemented or Interpreted Law: 63F-1-206**