DEPARTMENT OF ADMINISTRATIVE SERVICES
INTERNAL POLICIES AND PROCEDURES

300 **Employee Information Security**

Effective: December 3, 2013

References: DAS Enterprise Information Security Policy; DTS Security Policy 2.3 and 4000

Purpose:

Information security is of preeminent importance to the Department of Administrative Services (DAS). In response to an external security audit of all executive branch agencies, DAS created a policy of policies for information security tied directly to Department of Technology Services' (DTS) policies. Excerpts of those policies relating to DAS employee security responsibilities are included below. Following this policy will minimize security risks to the Department and protect the State's electronic information and technology assets.

Policy:

1. **Security Awareness and Training:** All new DAS employees and all contracted employees shall undergo Information System Awareness Training immediately upon being granted access to information systems and assets. Current DAS employees shall undergo Information System Awareness Training annually in order to maintain access to information assets. This training is available online at securityawareness.utah.gov.
2. **Media Protection:** DAS employees shall protect information system media, both paper and digital; limit access to information on system media to authorized users; and sanitize or destroy information system media before disposal or release for reuse in accordance with the guidelines set forth in DTS Security Policy. Employees shall only use State-owned *encrypted* media when downloading State data containing restricted or private information to a removable media device such as, but not limited to, USB drives, CDs, and DVDs.
3. **Personnel Security:** The Department shall ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions. In addition, the Department shall ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers and employ formal sanctions for personnel failing to comply with organizational security policies and procedures consistent with DTS Security Policy.
4. **Access Control:** Department information system access is limited to authorized users. Employees may not access, possess, or use restricted or private information for non-business needs including, but not limited to, commercial and personal use.
5. **Incident Notification and Response:** DAS employees shall report any security-related incident including suspicious activity or misuse of State systems to their supervisor and

notify DTS through the online incident notification form found at dts.utah.gov/security/. Suspicious activities include, but are not limited to:

a. Unauthorized access or changes to a system or data
b. Loss or theft of a device
c. Loss of confidential data
d. Unusual behavior of a device or system
e. Observation of an employee attempting to access a system with someone else's ID
f. Unknown persons tailgating into a restricted area
g. Defacement of a webpage

6. **Password Standards:** All Department administrative, supervisor, and user-level passwords shall conform to the guidelines set forth in DTS Security Policy as outlined below. Common, default or shared passwords are ineffective and aid hackers and others in their illicit attempts to access systems and confidential data with-in the State of Utah. Strong passwords play a critical role in protecting computers, systems, and data from unauthorized access.

    a. All user level passwords must be changed at least every 90 days. A user may not reuse the ten most recently used passwords. When changing a password it is not acceptable to simply add a number to the end of a previously used password (password88 to password89). Any time a user ID or password is suspected of being compromised the password must be changed immediately or a request made that the account be disabled.

    b. Strong password have the following characteristics:

        i. A password should be at least eight characters in length.
        ii. Passwords must not include any portion of your name, address, date of birth, Social Security Number, username, nickname, family name, pet name, sports team name or word that appears in a dictionary or any such word spelled backward.
        iii. Passwords must have a combination of letters, numerical digits and special characters.
        iv. Passwords must include at least one character from the four following attributes: uppercase letters (A-Z), lowercase letters (a-z), numeric characters (0-9), and special characters (i.e. !, @, #, $, %, ^, &, *).

7. **Mobile Device Management:** DAS employees using a mobile device, including a personal device, to access State restricted or private information are subject to DTS and DAS policies and all acceptable use standards.