State of Delaware
Department of Health and Social Services

EFFECTIVE DATE: October 17, 2014

POLICY MEMORANDUM NUMBER 3

Subject: Appropriate Use of DHSS Information Technology

I. Purpose

This document sets forth the DHSS policy on appropriate use of DHSS information technology. For the purposes of this document, DHSS information technology includes all hardware and software used as part of the duties of DHSS employees and contractual staff. This includes, but is not limited to, personal computing devices, servers, mainframe, telecommunications systems, data, files, applications, and the intranet and internet. The foundation of this policy is the Department of Technology and Information's DTI Acceptable Use Policy.

DHSS information technology is useful for acquiring and distributing information related to DHSS business and the delivery of services to DHSS clients. It is consistent with our efforts to improve coordination, collaboration, and learn from the experience of other agencies, as well as to share our own experiences. It is also consistent with our efforts to disseminate information about our services more effectively to our clients or potential clients.

It is expected that users will conduct State of Delaware business with integrity, respect and prudent judgment while upholding the state's commitment to the highest standards of conduct.

In addition, the purpose of this policy is to mitigate the risks associated with the use of this Department's information technology.

II. Scope

This policy applies to all users of DHSS information technology, regardless of the location from which it is being accessed. Further, this policy in conjunction with the DTI Acceptable Use Policy is intended to set expectations and boundaries for the appropriate use of DHSS information technology.

III. Definitions

Electronic Mail: Any communication transmitted via the intranet, internet or any other communication network (including wireless) used by the employee.
Portable Computing Devices: Any hardware that is designed to be moved frequently and used offsite or at alternate work locations. This includes laptops, PDA's, integrated messaging platforms, external storage devices including jump drives and

storage cards and any associated peripherals.

IV. Guidelines

A. **Use of DHSS Information Technology**: Employees must use DHSS information technology in a manner consistent with the DTI Acceptable Use Policy, IRM Organizational Policy and DHSS Policy Memorandum Number 5.
B. **Improper Use**: DHSS information technology shall not be used in a way that is disruptive, offensive to others, or harmful to morale. It is not permissible to use DHSS information technology for illegal purposes: to solicit or proselytize others for commercial ventures, religious or political causes, outside organizations, or other business related solicitations; to obtain or distribute computer games or chain e-mail. (See: Standards of Behavior; and DHSS Beliefs and Principles)
C. **The Use of Personal Computer (PC) Software**: Employees shall familiarize themselves and comply with DHSS Policy Memorandum Number 11.
D. **DHSS Rights**: All messages and files stored or transmitted on DHSS information technology are DHSS records. DHSS reserves the right to access and disclose all messages and files stored on its information technology or transmitted for any purpose. Users should have no expectation of privacy when using DHSS information technology.
E. **Privacy and Access**: For privacy reasons, employees are not permitted access to another employee’s computer files without the latter’s express permission. However, DHSS management reserves the right to access an employee’s computer files whenever there is a business need to do so and appropriate approvals acquired. (See Section VI - Monitoring of this document.)
F. **Securing Data and Files**: Employees using DHSS information technology shall take appropriate steps to safeguard the confidentiality of client and critical DHSS information Detailed client information may be transmitted through e-mail, but confidentiality, privacy and security requirements of the state, DHSS and the Health Insurance Portability and Accountability Act (HIPAA) must be followed. Data, especially client information, including that transmitted by e-mail, stored on portable computing devices, desktops, backup devices or stored on any other storage media must be protected at all times from unauthorized access, reproduction, distribution, etc. No client specific data should be stored on portable computing devices. Confidential or critical data stored must be encrypted and periodically reviewed. Files containing confidential data must be deleted or destroyed when no longer needed. Users are strongly encouraged to store these files in encrypted form on network drives to reduce the risk of unauthorized access. Seek guidance from your network administrators if you need assistance or guidance in enabling these features. (See: DHSS Policy Memorandum Number 5 and IRM Organizational Policy)
G. **Securing Workstations**: Users are responsible for securing their workstations and portable computing devices from unauthorized access at all times. Users must not leave their workstation unattended without securing it first. Workstations must be secured from unauthorized access by shutting down the computer, locking it from access by using Alt-Ctrl-Dlt, locking the door if in an

office or by activating a screen saver which locks it from access. DHSS computer equipment must not be moved from the primary work site without prior authorization. Workstations and portable computing devices authorized to be taken offsite must be protected from theft at all times. (See: IRM Organizational Policy)

H. **Internet/Intranet Access**: Users must comply with the DTI Acceptable Use Policy as it pertains to the internet. Users must not use the internet/intranet in an unsafe manner that could otherwise disrupt or threaten the viability of DHSS information technology. Users will not take actions that are in violation of website copyright and licensing agreements.

V. Notification

A. Warning Banner - DHSS will use the banner as set by DTI.

B. Signed Forms

C.The IRM Helpdesk is responsible for having a signed copy of the each of the following forms for each employee of the department:

1. DTI Acceptable Use Policy
2. DHSS User Non-Disclosure Agreement
3. DHSS Systems User Request Form
4. IRM Organizational Policy and DHSS Systems User Request Form Instructions

An annual review of the DTI Acceptable Use Policy is recommended by the Secretary of the Department of Technology and Information. This periodic review of the policy is the responsibility of each division.

VI. Monitoring

For information on monitoring, please refer to the IRM Organizational Policy.

VII. Non-Compliance

Failure to comply with any of the provisions of this policy and its procedures in any form could result in specific civil, criminal and/or Department penalties.

VIII. Implementation

A. This policy becomes effective immediately

B. This Department Policy supersedes all other Department policies, directives, or rules related to this subject.

Rita Landgraf, Secretary