DELAWARE HEALTH AND SOCIAL SERVICES

DHSS Policy Memorandum #3 **Effective: May 15, 2023**

Appropriate Use of DHSS Information Technology

I. PURPOSE:

The Department of Health and Social Services (DHSS) requires that all system users handle State of Delaware business with integrity, respect, and prudent judgment while upholding the State's commitment to the highest standards of conduct. The purpose of this policy is to mitigate the risks associated with the use of DHSS' information technology. 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, mobile devices, servers, mainframe, telecommunications systems, data, files, applications, and the intranet and internet.

II. SCOPE:

This policy applies to all permanent full-time, permanent part-time, contractual, temporary, limited term, casual, and/or seasonal employees of DHSS.

III. DEFINITIONS

Email: 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, mobile devices, external storage devices including external drives, thumb drives, and any associated accessories.

IV. POLICY:

All DHSS staff must use Information Technology (IT) in a manner consistent with State and DHSS policy including:

- DTI Acceptable Use Policy
- DHSS Non-Disclosure Agreement
- IRM Organizational Policy
- DHR Standards of Conduct

All messages and files stored or transmitted on DHSS IT are DHSS records. DHSS reserves the right to access and disclose all messages and files stored or transmitted on its IT for any purpose. Users have no expectation of privacy when using DHSS IT.

DHSS employees 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 keys simultaneously, locking the door if in an office or by activating a screen saver which locks it from access. Additionally, DHSS computer equipment and accessories 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.

DHSS employees are not permitted to access another employee's computer files without 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 have been acquired.

Employees using DHSS information technology must take appropriate steps to safeguard the confidentiality of client data and critical DHSS information. Detailed client information may be transmitted through secure email, but confidentiality, privacy and security requirements of the State, DHSS and the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 CFR Part 2, and 16 *Del. C.* § 1212 must be followed. Data, especially client information, including that transmitted by email, 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, and distribution. No client specific data is to 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.

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 must not take actions that are in violation of website copyright and licensing agreements.

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 others for commercial ventures, religious or political causes, or other solicitations, or to obtain or distribute computer games or chain e-mail.

The Information Resource Management (IRM) Helpdesk is responsible for having a signed copy of the each of the following forms for each DHSS employee:

- DTI Acceptable Use Policy
- DHSS User Non-Disclosure Agreement
- DHSS Systems User Request Form
- IRM Organizational Policy
- DHSS Systems User Request Form Instructions

Appropriate disciplinary action may be taken against any employee who violates this policy. Based on the seriousness of the offense, disciplinary action may include, but not be limited to, verbal reprimand, written reprimand, suspension, or termination of employment.

V. IMPLEMENTATION

This Policy Memorandum replaces previous versions of PM #3 and is effective upon signature of the Cabinet Secretary.

The Office of the Secretary will be responsible for maintaining this policy and any revisions.

Molly K. Magarik
Cabinet Secretary

5/31/2023
Date

The Department of Health and Social Services is committed to improving the quality of life of Delaware's citizens by promoting health and well-being, fostering self-sufficiency, and protecting vulnerable populations.