TO: DIRECTORS, LOCAL DEPARTMENTS OF SOCIAL SERVICES
DEPUTY/ASSISTANT DIRECTORS FOR FAMILY INVESTMENT
FAMILY INVESTMENT SUPERVISORS AND CASE MANAGERS
HEALTH OFFICERS, LOCAL HEALTH DEPARTMENTS
LOCAL HEALTH DEPARTMENTS, ELIGIBILITY STAFF

FROM: KEVIN M. MCGUIRE, EXECUTIVE DIRECTOR
CHARLES E. LEHMAN, EXECUTIVE DIRECTOR, DHMH, OOEP

RE: SYSTEM SECURITY REMINDER

PROGRAM AFFECTED: ALL PROGRAMS

ORIGINATING OFFICE: OFFICE OF PROGRAMS

Recently, several system security issues have come to our attention. Some of the issues include people sharing logon ID’s and passwords and unauthorized use of a coworker’s computer to finalize their own cases. When employees are hired, they sign a system software agreement. This agreement requires signers to acknowledge that they understand what will happen when infractions to system security occur (see the attached Employee Security Advisory form). This information memo is a reminder of the importance of DHR system security rules.

Sharing logon ID’s or passwords not only violates our system security rules, but also compromises case integrity. The CARES system is designed with software to ensure that two staff members touch every case for security reasons. Infractions to the process violate security requirements and complicate the tracking process.

If you have questions, please contact Stephanie Hawkins at shawkins@dhr.state.md.us or 410 767-8121.

cc: FIA Management Staff
    DHMH Management Staff
    Constituent Services
    DHR Help Desk
STATE OF MARYLAND
DEPARTMENT OF HUMAN RESOURCES – HRDT
EMPLOYEE SECURITY ADVISORY

This form is an acknowledgment of the responsibilities of employees in regard to the use of computer equipment, data, and software, including; mainframe computers, mini-computers, personal computers, either stand-alone or connected to local area networks (LANS), wide area networks (WANS), the Internet, an intranet, etc. Authorized access to and use of information and computer resources is limited to the PURPOSE for which these privileges are granted. Violation of this policy can result in disciplinary action including suspension and/or termination of employment. This advisory is initiated for informational purposes only. The following paragraphs shall in no way be construed as a waiver by an employee of the rights and protection provided to employees by the Merit System Law (State Personnel & Pension Article of the Annotated Code of Maryland).


Specifically, PROHIBITED ACTS include, but are not limited to:
1. Unauthorized access to or use of a computer, data, or software.
2. Unauthorized copying of software.
3. Use of unauthorized or unlicensed software.
4. Unauthorized obtaining, copying, or disclosure of confidential information.
5. Unauthorized modification to or altering of data or software.
6. Introduction of false information to public records.
7. Disruption or interruption of the operation of a computer.
8. Disruption of government operations or public services by means of a computer.
9. Unauthorized taking or destroying data or software.
10. Unauthorized creating / altering a financial instrument or fund transfer.
11. Misuse or disclosure of passwords and LOGON IDs.
12. Unauthorized breaching a computer security system.
13. Damaging, destroying, or the unauthorized altering / removal of computer equipment or supplies.
14. Devising or executing a scheme to defraud.
15. Obtaining or controlling money, property, information, or services under false pretenses.
16. Use of equipment, software, or data for other than the business of the State of Maryland.

All authorized users during the term of their granted access and thereafter, shall hold in strictest confidence and not willfully disclose to any person, firm or corporation without the express authorization of the Department of Human Resources Data Security Officer, any information related to security, operations, techniques, procedures, or any other automated system matter.

Any breach of security must be promptly reported to the Department of Human Resources, OIM Data Security Division, and the OIG.

I acknowledge that I have read and understand this security advisory.
Date: Signature:
Name (Print):
Date: Witness Signature:
Witness Name (Print):

DHR/HRDT 73 (3/00) RETAIN A COPY OF THIS DOCUMENT FOR YOUR RECORDS