DEPARTMENT OF WORKFORCE DEVELOPMENT
DIVISION OF ECONOMIC SUPPORT
ADMINISTRATOR'S MEMO SERIES

NOTICE 00-04

ISSUE DATE: 03/28/2000
DISPOSAL DATE: Ongoing

RE: COMPUTER SECURITY

To: Child Support Agency Directors
County Departments of Human Services Directors
County Departments of Social Services Directors
County Economic Support Managers/Supervisors
Tribal Chairpersons/Human Services Facilitators
Tribal Economic Support Directors
W-2 Agency Directors

From: Jennifer L. Noyes /s/
Administrator

Computer systems accessed by county/tribal agencies, W-2 agencies, child support agencies as well as state staff contain confidential or sensitive information. These systems, including but not limited to KIDS, CARES, EOS, LPMF, Wage records, Social Security records, IRS records, must be safeguarded.

Requests for information

Many local agencies are requested to verify information or provide copies of screens or reports to other agencies. While that may be permissible, every request should be questioned on two levels:

- Is the information requested, or is the purpose for releasing it, necessary for the Administration of the Programs (See Wis, Stat. 19.62 – 19.69 Personal Information Protection and 49.81 Public Assistance Recipient's Bill of Rights)?

- Is the person making the request who s/he says they are?

Every attempt must be made to verify there is a legitimate program need for the information and what the information will be used for. Then, and only then, should information be

provided. When you are unsure if information can be provided to the requestor, error on the side of caution. Do not provide it until the identity of the requester has been confirmed. It may be possible to confirm by return phone call or FAX the requested information to a known agency phone number. Do not provide confidential information via e-mail unless you have confirmed the e-mail address of the sender. Where information is shared on a regular basis, agencies should have data exchange agreements in place which spell out the business and legal need for the information, the specifics about what information will be shared, the conditions under which it will be shared, and the responsibility of the requesting agency to safeguard the information which is provided.

Even where there appears to be a legitimate program and legal need, there may be valid reason not to provide the information. An example of this is a request for data that we obtain from Social Security On Line Query (SOLQ). Our agreement with the Social Security Administration grants us access to the data for the specific purpose of eligibility determination relating to MA, Food Stamps and W-2. It does not cover providing that information to other agencies for their purposes. They would need to pursue their own agreement with the Social Security Administration in order to obtain access. Other data sources that our programs access on a regular basis include UI Wage Record information and IRS data. These data sources contain very sensitive information and agencies must make every effort not to allow that data to become known to anyone other than authorized staff.

Documentation of requests

Agencies should maintain a log of all requests for information, what staff person and agency requested it, date requested, phone/fax number of the individual/agency making the request, and the nature of the request. It may be necessary to have the requesting agency make their request in writing on their letterhead, stating what information is needed, why they need it and what it will be used for. Where information was provided verbally, the information provided should be documented in a log or in the case notes.

Best Practices for Safeguarding Information

The following are “best practices” to serve as examples for security of data:

- All information obtained through matches, either on-line or batch, should be independently verified prior to use.
- If using paper or printouts, items with client specific data should be secured when the user leaves the area. Any printout with confidential information (including screen prints) should be filed; it must be locked up. When they are discarded, they must be shredded.
- When providing hard copy print outs, each page should be clearly marked or stamped “CONFIDENTIAL”. This helps ensure proper handling, protection and disposition of hard copy material that contains sensitive personal information.
- When providing information on case participants, verify the identity of the person receiving the information and why they need the information. Document every request.
- Personal Computers must have password protected screen savers.
- Password protected screen savers must be invoked if you leave your workstation.

- ♦ Never give another person your password or allow them to use a device you have signed on.
- ♦ Agency security staff should make all staff aware of the following Memo's:

    - DES Administrator's Memo Series Notice 99-07
    - BWSP Operations Memo 00-07

- ♦ Agency security staff should make all staff aware of the following portions of the Security Manual (available via the DWD WorkWeb).

    [http://dwdworkweb/des/manuals/des/securman.htm]

- Chapter 03 – How to Create a Secure Environment
- Appendix 04 – Wisconsin Statutes 943.70
- Appendix 05 – DWD Security Policy
- Appendix 06 – Wisconsin Statutes Chapter 49

In summary, agencies need to ensure that reasonable and prudent procedures are in place to control access to information in order to the ensure the privacy of our participants.

REGIONAL OFFICE CONTACT: DES Area Administrator

CENTRAL OFFICE CONTACT: Thomas Meier
DES Security
608/266-7936