

Confidentiality, Disclosure and Data Security Requirements

Parties agree not to use or disclose information other than as permitted as agreed or required by law. The parties acknowledge that § 35A-4-312(7) imposes privacy and confidentiality requirements on information. Penalties, including criminal penalties under § 76-8-1301(4) Utah Code annotated, may be imposed for misuse or improper disclosure of such information. Under this agreement, the parties shall:

- A. have whole disk encryption on computers used for accessing or storing reports from the data;
 - B. limit access to its information using appropriate security controls in accordance with the most recent NIST 800-53 guidelines for transmitting, encrypting, storing, and maintaining DWS data: <http://www.nist.gov/publication-portal.cfm>;
 - C. only query information for individuals who are applying for or participating in Agency's programmed services;
 - D. have sufficient safeguards in place to ensure the information obtained is used only for the purpose stated in the agreement;
 - E. store and process information in such a way that unauthorized persons cannot retrieve the information by computer, remote terminal, or any other means;
 - F. identify all personnel, by position, authorized to request and receive information; and notify the other party of changes in authorization;
 - G. train authorized users accessing information under this MOU, on relevant statutes prescribing confidentiality and safeguarding requirements, disclosure prohibitions and penalties for unauthorized access or disclosure. Parties shall have the right to review disclosure training and request or suggest any changes necessary;
 - H. maintain each party's records only until such time that the records are no longer necessary and at that point, the records will be securely disposed of except for disclosed information possessed by any court. Disposal means return of the information to the other party or destruction of the information. Disposal includes deletion of personal identifiers by DWS in lieu of destruction. The information disclosed must not be retained with personal identifiers for longer than needed to fulfil the purposes of this agreement;
 - I. refrain from duplicating the provided records other than as required for disaster recovery; and
 - J. report any data breaches to the other party immediately on discovery and cooperate to mitigate any concerns.
- I. Monitoring
- Parties shall permit each other the right of a compliance review to ensure that the provisions of the agreement are upheld and will maintain a system sufficient to allow an audit of its compliance with the disclosure and confidentiality and access to data sections above.

II. Funds Accountability

The Deficit Reduction Act of 1984 requires that agencies utilizing income and eligibility verification systems provide reimbursement costs incurred by agencies in furnishing UI wage data under 42 USC 1320b-7(a)(7), 42 USC 503 and 20 CFR 603.08. It is presumed that the disclosure of information involves an incidental amount of staff time and no more than nominal processing cost and there is not a need for DAS to reimburse DWS for the information received. Exceptions to this provision will be negotiated between authorized individuals for each agency on a case-by-case basis consistent with 20 CFR 603.8 and 603.10.