Ohio Administrative Code

Rule 5101:9-9-37 Data system security.

Effective: July 1, 2021

The following requirements ensure the security of departmental data and must be followed by all county and state employees (hereafter referred to as 'user' or 'users') who access data systems maintained by the office of information services (OIS) and the Ohio department of job and family services (ODJFS) via the private or public network.

(A) Users are responsible for system inquiries and activities executed with their system user identification (USER-ID, also know as an Ohio ID, or OH|ID.)

(B) Users shall follow DAS password standards found at https://das.ohio.gov/portals/0/dasdivisions/employeeservices/pdf/das-its-2100-01-a das password standard organizational users.pdf.

(C) A terminal or personal computer must never be left unattended or unsecured when logged onto the ODJFS network or device.

(D) Only the files or information that are required to perform one's own job duties, shall be accessed.

(E) Users must comply with all items included on the user attestation, JFS 07078 " Code of Responsibility" form, and review and sign, electronically, on an annual basis.

(F) An original signed (physical or electronic) JFS 07078 hardcopy form, or digital JFS 07078 submission must be submitted to ODJFS with every county request for a USER-ID or user access to the OIS and ODJFS networks.

(G) The JFS 07078 (paper or digital form) is required for every new user accessing the system, and for making changes to an existing user's access.

(H) Counties must not modify the JFS 07078 form.

(I) County users shall also abide by the data security provisions contained in IPP 3001 found at ipp.odjfs.state.oh.us/IPP03000/.