General Rules of Behavior for Users Accessing Child Support Information

The following rules of behavior apply to all Department of Children and Families (DCF) employees, Child Support Agency (CSA) employees, and contractors who have access to child support information including Federal Tax Information (FTI).*

> * **Federal Tax Information (FTI):** Consists of federal tax returns and return information (and information derived from it) that is in the agency's possession and control. It is covered by the confidentiality provisions of the Internal Revenue Code and subject to Internal Revenue Code § 6103(p)(4) safeguarding requirements including IRS oversight. FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source such as the SSA-OCSS. FTI also includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source, such as a database like KIDS. FTI does not include copies of tax returns or return information provided directly by the taxpayer or the taxpayer's representative.

Per IRS Publication 1075 "Tax Information Security Guidelines for Federal, State, and Local Agency access to FTI" requires a signed acknowledgement annually indicating that you have read, understand, and agree to abide by the rules of behavior as outlined below. These rules are in addition to and not in lieu of any additional security restrictions the user has or will acknowledge acceptance of when working with FTI and/or child support information.

System Access

- I understand that I must complete mandatory security and privacy awareness training annually.
- I understand that I am given access only to those systems to which I require access in the performance of my official duties.
- I will not access systems and the data contained therein for any purpose other than conducting agency business.
- I will not attempt to access systems I am not authorized to access.

Passwords

- I will use strong passwords at all times that comply with the standards for the application.
- I will protect my passwords from disclosure at all times.
- I will not reveal my passwords to others and will not allow use of my accounts by others.
- I will promptly change a password if I suspect that my password has been compromised.

Data Access and Protection

- I will use only authorized equipment to access child support information, including FTI.
- I will protect sensitive information including FTI and PII from disclosure to unauthorized persons or groups.
- I will logoff or lock my computer whenever I step away from my work area, even for a short time. I will log out of any child support or other restricted application and log out of my workstation when I leave for the day.

- I will ensure proper handling and disposal of records containing sensitive information including FTI and PII, either in hardcopy, softcopy, or electronic media formats, according to policies and regulations which govern them.

Use of Agency Office Equipment

- I understand that agency office equipment is to be used for official use, with only limited personal use permitted as determined by agency policies and work rules.
- I understand that my use of agency office equipment may be monitored, and I consent to this monitoring.
- I will not download or install unauthorized software on agency equipment.
- I will not install or connect any unapproved hardware devices to agency equipment without proper authorization.
- I understand that I am responsible for the security of agency issued mobile devices and the data contained therein.
- I understand that all computers, electronic media, and removable media containing sensitive information must be kept under the protection and control of an authorized employee or when not in use, it must be securely stored. I understand all FTI must remain secured according to the standards outlined in IRS Publication 1075.
- I will promptly report if an agency issued mobile or any other electronic device is lost, stolen or damaged.

Use of the Internet, Email, Instant Messaging Tools, Cloud Collaboration Tools, and Social Media

- I understand that Internet activities which inhibit the security of agency information and information systems or impede the business function of the agency are prohibited.
- I will follow all agency policies and work rules with regard to use of the Internet, email, Voice over Internet Protocol (VoIP) phone systems, instant messaging and social media.
- I will not forward agency business specific information to my personal email account or use my personal email account to conduct agency business.
- I will not disclose sensitive agency information including FTI on social media/networking sites, on public websites, through instant messaging tools, or via any other unauthorized means.
- I will not disclose FTI in cloud-based collaboration tools including, but not limited to, Mural and Microsoft Teams.

Incident Response

Use of FTI for any purpose other than that authorized by the IRS is prohibited. Staff who observe possible improper use or disclosure of IRS information must take the following steps:

1. Report the incident to their supervisor.
2. Report the incident to BCS at DCFDLBCSIncident@wisconsin.gov.
    a. Contact the IRS Office of Safeguards via email at safeguardreports@irs.gov immediately but no later than 24 hours after identification of the possible issue involving FTI.

Staff may contact the IRS at the IRS email address above prior to notification of the state or their supervisor.

Acknowledgement Statement

I understand that failure to comply with these Rules of Behavior could result in oral or written warning, suspension or removal of system access, fines, criminal or civil prosecution, suspension from duty, termination of employment, or removal from a contract for contractor personnel.

I acknowledge that I have read, understand, and will comply with these Rules of Behavior.

_____	_____	_____
Employee Name	Employee Signature	Date Signed

As the above employee's supervisor, I certify that this employee has received the Rules of Behavior.

_____	_____	_____
Supervisor Name	Supervisor Signature	Date Signed