**Wisconsin Works (W-2) Agency Performance Assessment (WAPA)**

**Security Compliance Self-Assessment**

Personal information you provide may be used for secondary purposes [Privacy Law, s. 15.04(1)(m), Wisconsin Statutes].

The W-2 Agency/Contractor must email the completed form to the DCFMBDFESDataSteward@wisconsin.gov.

|  |
| --- |
| **W-2 AGENCY/CONTRACTOR INFORMATION** |
| Agency/Contractor Name |
| Primary Physical Location Address      |
| Date Self-Assessment Completed      |
| **SECURITY COMPLIANCE SELF-ASSESSMENT QUESTIONNAIRE** |
| **Record Keeping** |
| 1. | If physical paper containing state data is stored, how are the documents stored?      |
| 2. | **[ ]**  Yes [ ]  No [ ]  N/A Is physical paper containing state data stored at another (offsite) location other than the primary physical location? |
|  | a. | Please explain the physical location and security at the offsite location:      |
|  | b. | Please explain the process when requesting and receiving a document that is stored at an offsite location:      |
| 2. | How does the agency destroy physical paper containing state data?      |
| 3. | How does the agency destroy electronic media containing state data?      |
| **Physical Location Security/Secure Storage** |
| 1. | **[ ]**  Yes [ ]  No [ ]  N/A Are there areas in your physical location that only authorized staff have access to? |
|  | a. | If yes, please explain those areas:      |
|  | b. | If a W-2 Agency/Contractor with more than one physical location, explain if there are any notable differences from one location to the next location:      |
|  | c. | Explain the identification badge policy/process for staff:      |
| 2. | **[ ]**  Yes [ ]  No [ ]  N/A Are staff allowed to work at an alternate work site (for example, their personal residence)? |
|  | a. | **[ ]**  Yes [ ]  No If staff are allowed to work at an alternate work site, does the agency require prior approval? |
|  | b. | **[ ]**  Yes [ ]  No If staff are allowed to work at an alternate work site, does the agency complete an inspection? |
|  | c. | If the W-2 Agency/Contractor does not require prior approval or an inspection at an alternate work site, what policies are in place to safeguard state data when working at an alternate work site?      |
| 3. | **[ ]**  Yes [ ]  No Does the W-2 Agency/Contractor retain ownership of all hardware, software, and end-point equipment that receives, stores, processes, or transmits state data? |
|  | a. | If the answer is no, is the agency using a Virtual Desktop Infrastructure (VDI)? Please explain:      |
| 4. | What workstation policies/processes are in place to ensure state data is safeguarded?      |
| **Restricting Access** |
| 1. | **[ ]**  Yes [ ]  No Is access to state data restricted to only authorized staff who have a need to know? |
|  | a. | How is access restricted to only authorized staff? Please explain:      |
| 2. | **[ ]**  Yes [ ]  No [ ]  N/A Is state data disclosed to staff outside of the W-2 Agency/Contractor through a subcontractor(s)? |
|  | a. | List the subcontractor and their locations (please indicate if the subcontractor works at an alternate work site or at their residence):      |
|  | b. | **[ ]**  Yes [ ]  No Are the Data Sharing Agreements (DSAs) up to date?  |
| 3. | When working with state data, what is the email policy for the W-2 Agency/Contractor?      |
| 4. | When working with state data, what is the fax policy for the W-2 Agency/Contractor?      |
| 5. | **[ ]**  Yes [ ]  No Does the W-2 Agency/Contractor have a data incident reporting policy/process?  |
|  | a. | What is the incident reporting policy/process for the W-2 Agency/Contractor?      |
| 6. | **[ ]**  Yes [ ]  No Does the W-2 Agency/Contractor have a data breach policy/process?  |
|  | a. | What is the data breach policy/process for the W-2 Agency/Contractor?      |
| 7. | **[ ]**  Yes [ ]  No Does the W-2 Agency/Contractor prohibit offshore access to state data?  |
| 8. | Please explain how the W-2 Agency/Contractor demonstrates control of state data:      |
| **Computer System Security** |
| 1. | **[ ]**  Yes [ ]  No [ ]  N/A Does the W-2 Agency/Contractor require multi-factor authentication for remote access?  |
|  | a. | Please provide a description of the factors required and the implementation:      |
| 2. | **[ ]**  Yes [ ]  No [ ]  N/A Does the W-2 Agency/Contractor implement auditing procedures on agency/contractor owned systems? |
|  | a. | If yes, how long are records retained for?      |
| 3. | **[ ]**  Yes [ ]  No Does the W-2 Agency/Contractor perform monthly vulnerability scans?  |
| 4. | **[ ]**  Yes [ ]  No Does the W-2 Agency/Contractor maintain active vendor support for all devices on its network?  |
| 5. | How does the W-2 Agency/Contractor protect state data at rest on end-user computing systems (e.g., laptops, mobile devices, removal storage media)?      |
| 6. | **[ ]**  Yes [ ]  No Does the W-2 Agency/Contractor monitor, control and protect communications (e.g., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems?  |
| 7. | **[ ]**  Yes [ ]  No Does the W-2 Agency/Contractor implement cryptographic mechanisms to prevent unauthorized disclosure of state data during transmission (over the LAN and WAN) unless otherwise protected by alternative physical safeguards? |
|  | a. | Provide a description of any encryption used for physical protections for transmission lines:      |
| 8. | **[ ]**  Yes [ ]  No Does the W-2 Agency/Contractor identify, report, and correct system flaws timely?  |
|  | a. | Identify key tools that the W-2 Agency/Contractor uses to do this (e.g., System Center Configuration Manager, Tanium Patch Management):      |
| 9. | **[ ]**  Yes [ ]  No Does the W-2 Agency/Contractor provide up-to-date protection from malicious code at designated locations within organization systems.  |
|  | a. | Identify key tools that the W-2 Agency/Contractor uses to do this (e.g., Symantec Endpoint Protection, Microsoft Defender):       |
| 10. | **[ ]**  Yes [ ]  No Does the W-2 Agency/Contractor monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks? |
|  | a. | Identify key tools that the W-2 Agency/Contractor uses to do this (e.g., CrowdStrike, Splunk):      |
| **W-2 Agency/Contractor Point of Contact Information & Attestation** |
| I,     , in my role as the Point of Contact for , attest that by affixing my signature at the bottom of this document that has reviewed the security, confidentiality and safeguarded requirements of the Contract and Data Sharing Agreement and that we continue to be in compliance with the requirements. understands that the Department may make recommendations concerning security compliance and require that the W-2 Agency/Contractor take corrective action to remedy any identified deficiencies (e.g., Oral or written warnings, Corrective Action Plans, financial penalties as outlined in Appendix E, etc.) |
| Name      | Work Telephone Number      |
| Work Email      |
| **SIGNATURE** – Point of Contact | Date Signed      |

**DEFINITIONS:**

Data Incident1 means an occurrence that (1) actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that (2) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidental and inadvertent accesses are considered data incidents. Which means an incident involving the loss, theft, or inadvertent unauthorized disclosure of information or information systems containing state data. Not every incident may result in a data breach once it is determined.

Data Breach[[1]](#footnote-1) means a type of incident involving the loss, theft, control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for other than an authorized purpose. Which means an incident that involves sensitive, protected, or confidential information being copied, transmitted, viewed, taken, stolen, or used by an unauthorized individual without the knowledge or authorization of the owner.

Remote Access1 means access to an agency’s or organizational information system by an authorized user communicating through an external, non-organization-controlled network or computer (e.g., the internet) from a geographical distance or another location through a network connection.

State data means all tangible and intangible information, this includes, but is not limited to program information, Confidential Information, and Personally Identifiable Information (PII) for the purposes of administering a variety of programs to assist low income individuals and families to move towards self-sufficiency. These programs include, but are not limited to, Emergency Assistance (EA), Community Service Block Grants, Job Access Loan (JAL), Literacy and GED services, Refugee Cash Assistance (RCA), Refugee Medical Assistance (RMA), Skill Enhancement, Transitional Jobs (TJ), Transform Milwaukee Jobs (TMJ) and Wisconsin Works (W-2).

Confidential Information means all tangible and intangible information and materials accessed or disclosed in connection with this Agreement, in any form or medium (and without regard to whether the information is owned by the source agency or by a third party), that satisfy at least one of the following criteria:

* 1. Personally Identifiable Information (PII), as defined below;
	2. Non-public information related to the source agency’s staff, customers, technology (including data bases, data processing and communications networking systems), schematics, specifications, and all information or materials derived there from or based thereon;
	3. Information designated as confidential in writing by the source agency;
	4. Information prohibited from disclosure by federal law, including but not limited to the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232 & 34 CFR Part 99, and 42 CFR Part 2; and the Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Part 160 and part 164, Subparts A and E;
	5. Information prohibited from disclosure by Wisconsin statute, including but not limited to Wis. Stats. §§ 48.396 (court and law enforcement records), 48.78 (agency records about an individual who is or was in its care or legal custody), 48.981(7) (child protective services reports and records), 49.83 (public benefits information), 51.30 (treatment records), 118.125 (pupil records), 146.82 (patient health records), 938.396 (juvenile court and law enforcement records), and 938.78 (agency records about an individual who is or was in its care or legal custody).

Personally Identifiable Information (PII)means information that can be associated with a particular individual through one or more identifiers or other information or circumstances, including but not limited to the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in any manner that renders the element unreadable:

* 1. The individual’s last name on its own or in combination with the individual’s first name or first initial;
	2. The individual’s date of birth;
	3. The individual's Social Security number;
	4. The individual's driver's license number or state identification number;
	5. The number of the individual's financial account, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account;
	6. The individual's DNA profile; or
	7. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation, and any other information protected by state or federal law.
1. Sources: Federal Information Processing Standards (FIPS) 200, IRS Publication 1075, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 [↑](#footnote-ref-1)