**DET SYSTEM ACCESS REQUEST**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. User Employment Status:

DWD Employee? | [ ]  Yes | 1. Accounts Logon ID

      | [ ]  New User/Position(BIT-7712-E Submitted) | 1. Division

 | Other:      |
| 1. Bureau

      | 1. Unit

      |
| [ ]  No | 1. WIEXT ID (Self-Registration Required)

      | 1. Employer Name

      |
| 1. Employer Agency Type

[ ]  Workforce Dev Board [ ]  WDB Partner Agency [ ]  Data Recipient [ ]  Other:       |
| 1. Last Name, First Name AND M.I. of User

      | 1. Optional Display Name (Last Name, First Name)

      |
| 1. User Work E-mail Address

      | 1. User Work Telephone/FAX Number

(   )       Ext.       FAX (   )       |
| 1. Mother’s Maiden Name

      | 1. User Work Address

StreetCity, Zip | 1. Office Number

     | 1. WDA

 | 1. County

      |

1. REQUEST TYPE (Production environment only)

 [ ]  Update/Add User Access [ ]  Remove User Access [ ]  Inactivate User Access

New users: Box 13 is required Removes system/s checked in Box 19 All DET Systems access inactivated

1. DET SYSTEMS (\*) = Required field

 [ ]  ASSET \* Profile:

 Special Access Rights:

 [ ]  Hire Heroes [ ]  RES Mgmt [ ]  Workshop Staff

 [ ]  OVES Staff [ ]  RES Staff [ ]  Cust. Support (UI)

 [ ]  TESSA [ ]  TAA Creator

 [ ]  BASIS \* Profile:

 [ ]  cBASERS (YA) \* Role:

 \* Grantee(s):

 [ ]  COMET \* Profile:

 [ ]  ETPL \* Profile:

 (BWT staff only for ETPL Admin profile)

 [ ]  JCW Business \* Profile:

 (BJS staff only for JCWB Job Posting Mgt)

[ ]  MSFW (BJS staff only) \* Profile:

[ ]  RRETS \* Profile:

[ ]  SharePoint \* Access Level

 \* Site(s)

[ ]  SOLAR Profile

[ ]  UIBNET (UI authorization required)

[ ]  WI Fast Forward \* Profile:

[ ]  WOTC \* Profile

[ ]  Business Objects (BI):

 (Access restricted) \* Access Level:

 Data: [ ]  JCS Customer

 [ ]  JCS JCW Emp [ ]  Youth Apprenticeship

 [ ]  JCS Outcomes [ ]  Other (Specify in Box 20)

1. COMMENTS:

|  |  |  |
| --- | --- | --- |
| 1. Supervisor First and Last Name

      | 1. Supervisor E-mail Address

      | 1. Supervisor Work Telephone

(   )       Ext.       |
| 1. Supervisor Signature
 | Date Signed |
| 1. Authorizing Agency

      | 1. LSO/DSO First and Last Name

      | 1. LSO/DSO Telephone Number

(   )       Ext.       |
| 1. LSO/DSO Signature
 | Date Signed |

**Read carefully before signing this User Security Acknowledgement**

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

1. Data and its information content is a DWD asset which is required to be safeguarded in accordance with DWD Information Technology Policy 516.03 and WI Statutes 943.70 at <http://dwdworkweb/dwdpolicy/516_03.htm>.

2. DWD policy provides that (a) all passwords related to the legitimate access to data are personal to the operator authorized to access data and must be kept CONFIDENTIAL; (b) permitting another to use such password to gain access to data is expressly prohibited, and (c) an operator should never leave a workstation unattended without first terminating or locking their session.

3. A breach of DWD policy constitutes a security violation and may subject the operator to disciplinary action when circumstances warrant it. Any operator who knows of actual or attempted violations should notify his or her supervisor.

|  |  |
| --- | --- |
| 1. Signature of User Requesting Access
 | Date Signed |
| 1. DET Security Officer Signature
 | Date Signed |

**FORM INSTRUCTIONS**

# PLEASE follow the instructions below to successfully request access to DET systems and data.

* ALL fields (except Signature Fields 24, 28, 29, and 30) MUST be completed electronically using the fill-enabled fields.
* ALL users who require new or modified access to any of the state's automated data systems owned by the Division of Employment and Training (DET) MUST complete and submit this form.
* Supervisor Signature MUST be present to request access, and User Signature MUST be present before DET will release User Accounts (logons/passwords) for DET System/Data access.
* For Non-DWD staff, ALL completed forms MUST be authorized by the User's designated Authorizing Agency and MUST be signed and submitted by a Local Security Officer (LSO) of record.
* For DWD Non-DET staff, ALL completed forms MUST be signed and submitted by a Division Security Officer (DSO).

ALL authorized forms are to be submitted via e-mail to the DET Security Unit: DETSecurity@dwd.wisconsin.gov

Questions? Email DET Security: DETSecurity@dwd.wisconsin.gov

**Supervisor responsibilities:**

* Make sure Fields 1-23 are completed fully and accurately to designate appropriate access based on the User's position/role, and limit access to information needed for work tasks ONLY. Make sure Fields 25-27 are completed, as needed.
* Make sure the User reads and understands the User Security Acknowledgement and signs the form in Field 29.
* Authorize User access via signature in Field 24.
* Submit form to LSO/DSO for authorization and processing. NOTE: ONLY DET Supervisors may submit directly to DET Security.
* Notify designated Authorizing Agency LSO or DSO of User's change in employment status or role where modification of Update, Add, Remove or Inactivate status of User account(s) is required.

**Local Security Officer (LSO) and Division Security Officer (DSO) responsibilities:**

* Verify the form has been filled electronically, ALL information is complete and valid, the requested access is appropriate, and both User and Supervisor Signatures are collected.
* Authorize access via signature in Field 28.
* Submit form to DET Security Unit for processing.
* Notify the DET Security Unit of User's change in employment status or role where modification of Update, Add, Remove, or Inactivate status of User account(s) is required. Notify the DET Security Unit of any change in Supervisor.
* Monitor User access to assure compliance with security standards and rules per User Security Acknowledgement, DSA, agency policy, Wisconsin Statutes and/or Federal law as applicable.
* Notify DET Security Unit immediately in the event of a security violation or a need to Remove or Inactivate User account(s) status.

**DET Security Unit is ultimately responsible for the authorization of all requests. Once authorized:**

* Update, Add, Remove or Inactivate User account status, and Add or Remove DET System/Data User access as appropriate.
* Form is signed by the DET Security Officer in Field 30, and securely stored per Records Disposal Authorization (RDA).
The form remains on file until for 24 months after the date the User account is in Inactivate status.
* Notify the LSO/DSO, User, and (optionally) User's Supervisor, as appropriate.
* If the access request is denied, DET Security Unit will notify the LSO/DSO (or DET Supervisor) of the reason.
The form will be destroyed without being processed.

DET System Access support is available be sending an email to the Applications Support mailbox: detAppsSupport@dwd.wisconsin.gov

* Staff assistance for ASSET, BI Launch Pad, JCW Business

REMEMBER – PASSWORDS ARE NOT TO BE SHARED WITH ANYONE!

DO NOT WRITE THEM DOWN OR POST THEM ANYWHERE WHERE OTHERS CAN SEE.

**FORM FIELD COMPLETION INSTRUCTIONS**

**If User is a DWD Employee:**

* Field 1: Check Yes. Fields 2-5: Enter the Accounts Logon ID and identify the Division/Bureau/Unit. Proceed to Field 9.
* For a new employee: Leave Field 2 blank. Check the New User box. Submit BIT-7712-E DWD Logon ID Request.
NOTE: Leave Field 11 blank (User Work E-mail Address). After the BIT-7712-E has been processed, DET DSO completes the fields.

**If User is NOT a DWD Employee:**

* The user MUST self-register and create a WIEXT account at https://accounts.dwd.wisconsin.gov.
When creating the WIEXT account, the user MUST include a work e-mail address and work telephone number.
* Field 1: Check No. Fields 6-8: Enter the WIEXT ID, Employer Name, and Employer Agency Type. Proceed to Field 9.

**ALL Users:**

Fields 9-17: Enter the remaining User Identification. Field 18: Check Request Type. Field 19: Select from DET Systems.
Field 20: Add Comments. Complete these fields as needed to identify DET System/Data needed to support the User position/role.

Field 24: A Supervisor Signature is required before DET Security will take any action on submitted requests.

Field 29: ALL Users MUST sign User Security Acknowledgement before User account(s) are released for DET System/Data access.