


Policy Title:		User Account Management Policy	
	OFFICE OF THE CHIEF INFORMATION OFFICER	Category	IT User Accounts
		Administrative Policy #	
		Revision #	N/A
		Review Frequency	As Needed – no less frequently than triennially
Administrative Division	Information Technology Services (ITS)	Reviewed By	Chief Information Officer
BOWC Approval		Last Reviewed/Update Date	7/2/19
Implementation Date			

1. OBJECTIVES

- 1.1. To ensure that all new, returning, transferring, or terminated DWSD employees and contractors are provided the correct information technology access to ensure their job needs are met.

2. PURPOSE

- 2.1. This process encompasses the complete life cycle of a user account including creation, maintenance, deactivation, and disposal. Familiarity with the application interface is assumed throughout the document.

3. DEFINITIONS

“Contractor/Vendor” means any third party company or individual who has access to DWSD’s IT environment.

“Deactivate” means to remove a user from all systems.

“Disable/terminate access” means to prevent a user from authenticating to systems. This is typically a temporary measure.

“Enable/allow access” means to allow a user to authenticate to systems.

“User ID” means generated unique user identifier used for authentication.

4. SCOPE

- 4.1. This policy applies to all DWSD employees, as well as any outside contractors/vendors that have access to DWSD’s IT environment.

5. RESPONSIBILITIES

5.1. Information Technology Services (“ITS”)

- 5.1.1. ITS is responsible for administration and oversight of this policy.

5.2. Employees, Contractors and Vendors

- 5.2.1. Responsible for ensuring they are in compliance with this policy.

6. POLICY

6.1. Addition/Modification/Termination

- 6.1.1. A Manager may request the addition/modification/termination of any employee/contractor/vendor.
- 6.1.2. Human Resources must be copied on any request and must approve any addition/modification/termination request of an employee. HR will communicate approved requests to ITS.

6.2. User ID

- 6.2.1. Each user must be provided with a unique information system identifier (User ID).

6.3. Granting of Access

- 6.3.1. Granting of access will follow the principle of least privilege (POLP), which is the practice of limiting access rights for users to the bare minimum needed to perform their work.

6.4. Use of Shared Accounts

- 6.4.1. Shared accounts are not allowed, unless there is documentation and approval by ITS as to why the exception is required.

6.5. Login

- 6.5.1. Each vendor/contractor is required to have a unique login for each user.

6.6. Revoking of Access

- 6.6.1. Revoking of access for terminated employees/contractors/vendors will occur on the date noted on a Separation Request.
- 6.6.2. Access for involuntary terminated employees must be revoked immediately upon notification. The terminating party and/or application manager should notify ITS in advance to coordinate efforts.

6.7. Identity Management

- 6.7.1. ITS will maintain a central user registry for all employees and contractors that will serve as a central store for IT-related identity and account information.

6.8. User Account Access Review

- 6.8.1. User account access should be reviewed at least once a year by ITS and related business partners to ensure users don't have access beyond their job responsibilities (least privilege). This review should include the specific rights/privileges, as well as elevated privileges of current users for each system to ensure accuracy and appropriateness. Documentation of these reviews will be retained by ITS.

6.9. Vendor or Default User Accounts

- 6.9.1. All default user accounts will be disabled or changed. These accounts include "guest", "temp", "admin", "Administrator", and any other commonly known or used default accounts, as well as related default passwords used by vendors on "commercial off the shelf" systems and applications.

6.10. Test Accounts

- 6.10.1. Test accounts can only be created if they are justified by the relevant business area or project team and approved by the application owner, through a formal request.
- 6.10.2. Test accounts must have an expiry date (maximum of 6 months). Maintaining test accounts beyond this date must be re-evaluated every 90 days and approved appropriately.
- 6.10.3. Test accounts will be disabled and deleted when they are no longer necessary.

6.11. Reasonable and Necessary Accommodations

- 6.11.1. Management may take reasonable and necessary actions to accomplish the intent of this policy.

7. PROCEDURE

7.1. Granting Access – Regular Employee. A supervisor/manager notifies Human Resources in writing the intent to add a new employee.

- 7.1.1. Once notified, Human Resources submits a ticket to the IT Service Desk to notify IT of the new employee.
 - 7.1.1.1. The ticket will include the new employee's first name, the new employee's job title and the start date. In addition, this will include any IT application access the employee will need outside of Active Directory and the level of access needed.
 - 7.1.1.2. All employees will be provided an email address.
- 7.1.2. The Service Desk sets up a parent ticket using the new employee template already created within the system that generates child tickets to ensure all access is granted and all materials/property are assigned.
- 7.1.3. The child tickets are automatically routed to IT personnel responsible for granting IT user access and granting IT related materials/property. These tasks will be completed prior to the start date noted in the submitted parent ticket.
 - 7.1.3.1. Each user will be provided with a unique information system identifier (User IDs). Examples of identifiers include user IDs and employee numbers. Additionally, the user will be provided with a unique information system authenticator that is tied to the assigned identifier. Examples of authenticators include passwords and tokens. Identifiers and authenticators will be delivered to the authorized user in such a manner as to ensure they are received only by the authorized user. To minimize risk, identifiers and authenticators for critical information systems will not be provided together.
 - 7.1.3.1.1. User IDs should be constructed in one of the following manners:
 - 7.1.3.1.1.1. Contractors/Vendors: Company identifier, last name, first initial
 - 7.1.3.1.1.2. DWSD Employees: Last name, first initial and middle initial
 - 7.1.3.2. Authenticators must be unique to each individual and to each system; however, a master authenticator may be used to access individual system authenticators (a single sign-on system). The authenticator must adhere to the Password Policy.

7.1.3.3. The identifiers and authenticators associated with each account must be distributed in such a manner as to ensure they are delivered only to the personnel to whom they are assigned:

7.1.3.3.1. Identifiers are to be distributed in a manner that eliminates repudiation of receipt.

7.1.3.3.2. Authenticators are to be distributed in a manner that protects their secrecy and eliminates repudiation of receipt.

7.1.4. Granting of access will include Active Directory and all applications that are applicable to the employee's role. This will also include any elevated privileges within each application and the network. Granting of access will follow the rule of least privilege. If elevated privileges are needed, a separate and individual privileged user account must be created.

7.2. Granting Access – Contractor/Vendor. Once the contract has been signed, the contract manager submits a ticket to the IT Service Desk to notify IT of the contractors/vendors that require access.

7.2.1. The ticket will include the new contractor/vendor's first name, the new contractor/vendor's job title and the start date. In addition, this will include any IT access the contractor/vendor will require.

7.2.1.1. Business Partners who wish to provide access to DWSD applications or provide DWSD email addresses to vendors or contractors must identify a funding mechanism (i.e., ITS has not factored these items into a budget and, thus, should be considered as part of a project budget within the business unit).

7.2.2. If there will be multiple individuals from one contractor/vendor that will require IT access, each individual is required to have his/her own user account and login.

7.2.3. Procedures from 7.1.2 apply from this point on.

7.3. Modification of User Access. A supervisor/manager notifies Human Resources in writing regarding the change of an employee's position.

7.3.1. Once notified, Human Resources submits a ticket to the IT Service Desk to notify IT of the change.

7.3.1.1. The ticket will include the employee's first and last name, the employee's new job title, the employee's old job title and the effective date of the change. In addition, this will include any IT access the employee will need outside of Active Directory or a similar job role that could be copied.

7.3.2. The Service Desk sets up a parent ticket using the new employee and terminated employee template already created within the system that generates child tickets to ensure all access is granted and revoked as necessary.

7.3.3. The child tickets are automatically routed to IT personnel responsible for granting and revoking IT user access. These tasks will be completed prior to the start date noted in the submitted parent ticket.

7.3.4. Revoking of access should include all applications that are applicable to the employee's access rights for their old role. This should also include any elevated privileges within each application and the network.

- 7.3.5. To maintain the requirements of least privilege, all accounts must first be disabled, privileges removed, then accounts re-enabled and privileges added.
- 7.3.6. The IT personnel assigned to the task will document in the ticket what access was granted/revoked and when.
- 7.3.7. Once the task from the child ticket has been completed and access has been granted/revoked, the IT personnel assigned to this task will set the status of the child ticket to completed and close it.
- 7.3.8. Once all child tickets have been completed and closed, the Service Desk will close the parent ticket and notify Human Resources that the ticket has been completed and closed.
 - 7.3.8.1. ITS will execute Service Desk tickets by the due date noted. Human Resources should monitor timely completion and escalate matters to ITS when necessary.
- 7.3.9. To ensure that all access associated with the employee's old role has been revoked, IT personnel will review all applications to ensure the employee no longer has access to those not needed, including elevated privileges.

7.4. Termination – Regular Employee.

- 7.4.1. Human Resources submits a ticket to the IT Service Desk to notify IT of an employee termination.
 - 7.4.1.1. The ticket should include the full name of the employee terminated, the supervisor/manager, and the termination date.
- 7.4.2. The Service Desk sets up a parent ticket using the termination template already created within the system that generates child tickets to ensure all access is revoked and all materials/property are returned.
- 7.4.3. The child tickets are automatically routed to IT personnel responsible for revoking IT user access and collecting IT related materials/property. These tasks will be completed by the end of the next calendar day following the termination date noted in the submitted parent ticket unless stated otherwise.
 - 7.4.3.1. Revoking of access should include Active Directory and all applications that are applicable to the employee's access rights. This should also include any elevated privileges within each application and the network.
 - 7.4.3.2. One of the child tickets will show a listing of all applications the employee was given access to during the onboarding process, and this will be used as a guide for revoking application access for the terminated employee outside of Active Directory. This information will be routed to each application owner, and it is their responsibility to ensure access has been revoked from those applications that are applicable.
 - 7.4.3.3. All user IDs and passwords for the terminated employee will be reset.
 - 7.4.3.3.1. Shared passwords will be changed within 30 days of termination date.
 - 7.4.3.4. All applicable user certificates will be revoked.

7.4.3.5. User profiles will be deleted unless there is a reason documented as to the need to keep the profile for archiving purposes. If it is determined that the user profile will not be deleted, the user profile must be disabled.

7.4.3.5.1. This status will be reviewed on an annual basis as part of the annual user access review to ensure that disabled user profiles still need to be archived.

7.4.4. The IT personnel assigned to the task will document in the ticket what access was revoked and when.

7.4.5. Once the task from the child ticket has been completed and access has been revoked, the IT personnel assigned to this task will set the status of the child ticket to completed and close it.

7.4.6. Once all child tickets have been completed and closed, the Service Desk will close the parent ticket and notify Human Resources that the ticket has been completed and closed.

7.4.6.1. ITS will execute Service Desk tickets by the due date noted. Human Resources should monitor timely completion and escalate matters to ITS when necessary.

7.5. Termination – Contractor/Vendor. The contract owner submits a ticket to the IT Service Desk to notify IT of the end date of the contract to ensure the contractors are not given access beyond the contract terms.

7.5.1. The Service Desk sets up a ticket to ensure all access is revoked and all materials/property are returned. The ticket is assigned to the appropriate IT personnel responsible for revoking contractor/vendor access. These tasks will be completed by the end of the next calendar day following the termination date of the contract.

7.5.1.1. Revoking of access should include Active Directory and all applications that are applicable to the contractor/vendor access rights. This should also include any elevated privileges within each application and the network.

7.5.1.2. All user IDs and passwords for the terminated contractor/vendor will be reset.

7.5.1.2.1. Shared passwords will be changed within 30 days of termination date.

7.5.1.3. All applicable user certificates will be revoked.

7.5.1.4. User profiles will be deleted unless there is a reason documented as to the need to keep the profile for archiving purposes. If it is determined that the user profile will not be deleted, the user profile must be disabled.

7.5.1.4.1. This status will be reviewed on an annual basis as part of the annual user access review to ensure that disabled user profiles still need to be archived.

7.5.2. The IT personnel assigned to the task will document in the ticket what access was revoked and when.

7.5.3. Once the task from the ticket has been completed and access has been revoked, the IT personnel assigned to this task will set the status of the ticket to completed and close it. The IT personnel will contact the project manager to let them know the ticket has been completed.

7.5.3.1. ITS will execute Service Desk tickets by the due date noted. The project manager should monitor timely completion and escalate matters to ITS when necessary.