Procedures for Application Security

This document outlines the procedures for obtaining and removing access for the following:

- NWRDC User ID Admissions
- Data
- myFSU BI (Legacy Student Data)
- Centralized Address System
- Counseling Center
- FSU Identity Applications
- Financial Aid
- Health Center
- Housing
- Orientation
- Student Academic
- Student Financial/Cashiering
- Withdrawals

To Acquire a NWRDC User ID for an Employee

A NWRDC User ID is required to obtain access for the following systems:

- Admissions Data
- myFSU BI (Legacy Student Data)
- Counseling Center
- Health Center
- Housing
- Orientation
- Student Academic Data
- Student Financial/Cashiering
- Withdrawals

1. The Supervisor will:
   - Consult with the Departmental Security Coordinator (DSC) to determine the access needs of the employee.

2. The Supervisor or DSC will:
   - Request the FSU_NWRDC_ACCOUNT role via the eORR application in OMNI.

3. The Employee will:
   - Utilize eORR workflow and digitally sign the confidentiality statement.

4. The Supervisor will:
   - Utilize eORR workflow to approve (or deny) the role request.

5. ITS Application Security will:
   - Provision the account at NWRDC.

- Utilize eORR to communicate to the employee and supervisor that the account has been created and to provide further instructions, if applicable.

To Acquire Application-Specific Access for an Employee

The following steps outline the process for acquiring access to the various applications listed at the beginning of this document. The following applications require a NWRDC User ID before access can be granted.

- Admissions Data
- myFSU BI (Legacy Student Data)
- Counseling Center
- Health Center
- Housing
- Orientation
- Student Academic Data
- Withdrawals

1. The Supervisor will:
   - Consult with the Departmental Security Coordinator (DSC) to determine the access needs of the employee.

2. The Supervisor or DSC will:
   - Complete the appropriate sections of the “Computer System Application Access Form”.
     - The “Employee Information” section contains information about the grantee including information required for positive identification.
     - The “Application Request Information” section is used to indicate the application(s) for which the request is intended.
       Note that additional forms, if required, must accompany the “Computer System Application Access Form” for access to be granted.

3. The Employee will:
   - Read and sign the “Employee Acknowledgement” section of the form.

4. The Supervisor and DCS will:
   - Sign the “Supervisor and DSC Approval” section of the form.

5. The Supervisor, DSC, or Employee will:
   - Fax the completed form and any additional forms to the appropriate Application Security Manager at the number(s) provided on the form.

6. The ASM will:
   - Approve or deny the access request based on a need to know.
   - Notify the appropriate DSC or supervisor of the decision.

To Change Access

It is the responsibility of the Supervisor to determine what access an employee requires to complete their documented job tasks and requirements. Supervisors should take immediate action to remove unnecessary access should job tasks or responsibilities change.

1. The Supervisor or DSC will:
   - Complete the appropriate sections of the "Computer System Application Access Form" form.
     - The "Employee Information" section contains information about the grantee including information required for positive identification.
     - The "Application Request Information" section is used to indicate the application for which the request is intended. Check the "Add" next to each application which is to be added to the employee's authorized access. Check the "Delete" box next to each application which is to be removed from the employee's authorized access.
       Note that additional forms, if required, must accompany the "Computer System Application Access Form" form for access to be granted.

2. The Employee will:
   - Read and sign the "Employee Acknowledgement" section of the form.

3. The Supervisor and DCS will:
   - Sign the "Supervisor and DSC Approval" section of the form.

4. The Supervisor, DSC, or Employee will:
   - Fax the completed form and any additional forms to the appropriate Application Security Manager at the number(s) provided on the form.

5. The ASM will:
   - Approve or deny the access request based on a need to know.
   - The ASM will perform the appropriate steps to remove or add access to the application(s) and notify the DSC or supervisor of the steps taken.

To Acquire a Access to FSU Identity Applications

There are several levels of security access available in the FSU Identity Applications. Requests for gaining or removing access to these applications are done in the eORR application in OMNI. All levels of security require justification for access. The justification should be specific about the job duties that require the access to the application. The roles available are described below.

- FSUID Lookup
  - FSU_FSUID_LOOKUP_DEPT role: Read-only access to the same data as the former FSUID Helpdesk application with the exception of data expressly deemed private by law or individual. Default access is for current department only.
  - FSU_FSUID_LOOKUP_CAMPUS role: Read-only access to the same data as the former FSUID Helpdesk application with the exception of data expressly deemed private by law or individual. This role is for campus-wide access. This role will require justification. The justification should be specific about the job duties that require campus-wide access to the application.

- FSUID Helpdesk
  - FSU_FSUID_HELPDESK_DEPT role: Access to the same data and functionality as the former FSUID Helpdesk application with the exception of data expressly deemed private by law or individual. This application allows the user to reset passwords, associate AD accounts, and rebuild FSUID for other individuals. Default access is for current department only.
  - FSU_FSUID_HELPDESK_CAMPUS role: Access to the same data and functionality as the former FSUID Helpdesk application with the exception of data expressly deemed private by law or individual. This application allows the user to reset passwords, associate AD accounts, and rebuild FSUID for other

individuals. This role will require justification. The justification should be specific about the job duties that require campus-wide access to the application.

- FSUID Trusted Lookup
    - FSU_FSUID_TRUSTED_LOOKUP_CAMPUS role: Read-only access to the same data as the former FSUID Trusted Helpdesk. This application includes data expressly deemed private by law or individual and is for use by the FSU Police Department. Default access is campus-wide. This role requires justification. The justification should be specific about the job duties that require the access to the application.

- FSUID Secure Identity Lookup
    - FSU_FSUID_LOOKUP_SECURE_CAMPUS role: This application is used for reconciling identity information. Default access is campus-wide. This role requires justification. The justification should be specific about the job duties that require the access to the application.

- FSUID Network
    - FSU_FSUID_NETWORK_DEPT role: Read-only access to the same data as the former FSUID Network application with the exception of data expressly deemed private by law or individual. This application allows the user to view and modify FSU WIN status for their current department.
    - FSU_FSUID_NETWORK_CAMPUS role: Read-only access to the same data as the former FSUID Network application with the exception of data expressly deemed private by law or individual. This application allows the user to view and modify FSU WIN status. Default access is campus-wide. This role will require justification. The justification should be specific about the job duties that require campus-wide access to the application.

The steps for acquiring access are as follows.

1. The Supervisor will:
    - Consult with the Departmental Security Coordinator (DSC) to determine the access needs of the employee.

2. The Supervisor or DSC will:
    - Request the appropriate FSUID role via the eORR application in OMNI. Written justification is required for access to these applications. The justification should be entered in the “Comments” box on the eORR role request.

3. The Employee will:
    - Utilize eORR workflow and digitally sign the confidentiality statement.

4. The Supervisor will:
    - Utilize eORR workflow to approve (or deny) the role request.

5. ITS Application Security will:
    - Provision the account at NWRDC.
    - Utilize eORR to communicate to the employee and supervisor that the account has been created and to provide further instructions, if applicable.

Terminations

The NWRDC role will be removed automatically from an employee after their termination date. To remove the role prior to the employee's last day, the Supervisor or DSC should use the eORR application in OMNI to request removal of the role. It should be noted that assigned NWRDC User IDs are never terminated (destroyed) or reassigned to another employee to preserve history and accountability. The accounts are inactivated and cannot be used to log onto any online system at NWRDC.

When an employee who has been assigned a NWRDC User ID submits a resignation terminating employment with the department/division or University, the supervisor should immediately review all of the access that employee and notify the DSC.

1. The Supervisor or DSC will:
   - Complete and sign the "Computer System Application Access Form" form. Indicate the date access should be terminated in the "Employee Information" section on the form (e.g. Access Termination Date: 6/30/2010).
   - Fax the completed "Computer System Application Access Form" to the appropriate Application Security Manager at the number(s) provided on the form.

When an employee has been terminated from OMNI and there are no other active appointments, the eDIR process will remove the NWRDC Account role in OMNI. It is the responsibility of the ITS Application Security team to deactivate the account when the role is removed.

2. ITS Application Security will:
   - Run a daily query to review inactive employees to ensure their NWRDC Account roles are removed.
   - Deactivate the users' NWRDC IDs identified by the query.
   - Advise the DSC and supervisor of the deactivation.

Attestation Process

ITS Application Security has several business processes in place to audit role assignments for various accounts and applications.

ITS Application Security:

- Reviews a daily report of inactive employees that have an active NWRDC role.
- Reviews a daily report of department changes for employees and work with the Employee, DSC, and the Employee's Supervisor to determine if access changes are necessary.
- Provides quarterly reports for OMNI roles.
- Provides and maintains OMNI queries for supervisors and Departmental Security Coordinators to use as needed.