Compliance Procedure

Title: **Account Management Procedure**
Reference Number: **5.2.2**

Purpose
This procedure provides guidance on how computer accounts are to be created, maintained and terminated at Old Dominion University.

Scope
This procedure pertains to all network and IT computing accounts, managed by OCCS, that are used for conducting the business of Old Dominion University or on which sensitive data resides or is transmitted.

Requesting an Account –

Accounts at Old Dominion University are requested in one of two basic ways. Some accounts and services are requested on-line through the MIDAS application. Other accounts and services are requested by completing a Universal Account Request form.

MIDAS Account Request – https://midas.odu.edu/
Members of the University community are eligible for a MIDAS account by having a basic person record in the Banner system. Information from Banner is used to verify their identity and determine their role(s) with the University. Based upon their role and the eligibility rules established by the System Owners, accounts and/or services are either automatically created or are optional and may be activated by the end user.

Upon initial login, MIDAS requires the user to accept the Acceptable Usage Policy, take one or more role based Security Awareness training courses on-line, create a secure password and create a security profile that is used for managing the lost & forgotten password process. Only after these requirements have been met are accounts and services made available.

Universal Account Request Forms – http://occs.odu.edu/forms/acctreqform.pdf
Some accounts and services require a higher level of approval and authorization. Examples of accounts that require the Universal Account Request form are Banner, faculty/staff E-Mail and LAN, Web Time Entry and others. The form should be filled out completely. The requester must sign the Acceptable Usage Statement. If the account is being requested by a person that is not already in Banner, the full name, date of birth and gender must also be collected so that a basic person record can be created in Banner by the Human Resources department.

Application Specific Account Request Form – http://occs.odu.edu/page.php?page=about/forms
There may exist specialized forms unique to the needs of specific applications. These forms verified and processed in the same manner as the Universal Account Request form.

Account Authorization –

MIDAS Account Request –
To the extent possible, the authorization decisions for accounts and services made available through MIDAS are automated and are based upon information in Banner and pre-approved by the System Owners.

Universal Account Request Forms –
System Owners and/or Data Owners must approve access to the systems/data they own. Employees must also receive the approval of their Budget Unit Director (BUD) for accounts/services they need for

the performance of their job. The signatures must be obtained prior to sending the completed form to the OCCS Account Manager for processing. Accounts will not be created without proper authorization signatures.

Creating Accounts –

MIDAS Account Request –
After the training, AUP, Security Profile and any other prerequisites are completed, the MIDAS application creates accounts in constituent systems via connectors that interfaces between MIDAS and the target system. The account is created, verified and recorded in the Accounts Tracking System (ATS). The status of the account(s) is available to the user through the MIDAS 'My Services' screen. MIDAS does extensive logging to assist in problem resolution and process auditing.

Universal Account Request Forms –
Account forms are received by the OCCS Account Manager and recorded in the Footprints application as being received. The OCCS Account Manager reviews the form.

Incomplete forms are returned to the requester to complete. Forms missing authorization signatures are sent via the campus mail to the approvers for signature. Copies may be made to expedite the process. The approvers returned the signed forms to the OCCS Account Manager via campus mail.

The requested accounts are documented in Account Tracking and follow one of three basic creation processes:

Simple Internal Account Creation Process –

Simple accounts are authorized via the Account Request form but created and maintained via MIDAS. Examples of this type of account are ODUNet and Banner Web Proxy. The Account Manager synchronizes MIDAS with ATS, which creates and maintains the accounts.

Internal Account Creation Process –

Internal Accounts are authorized via the Account Request form but the Accounts Manager uses a secondary application to enable the account for use. Examples of this type of account are faculty/staff Lotus Notes and faculty/staff LAN. The Account Manager manually creates the account in the constituent system. If the application has been 'integrated' with MIDAS, the Account Manger will synchronize the password and account status with MIDAS.

External Account Creation Process –

External accounts are authorized via the Account Request form, documented by the Accounts Manager but created by a System Administrator or Data Custodian. Examples of this type of account are UNIX accounts and Oracle Academic database accounts. The Accounts Manger adds the System Administrator/Data Custodian to the footprints ticket and gives the request form to them for account creation. The form and any deliverables are returned to the Account Manager once the account is created.

The Account Request forms are filed in the Account Managers office and the Footprints ticket is closed. The end user is notified that the account is created and any special instructions that are needed.

Changes to Accounts and Access –

General Changes –
Changes are considered to be access or attribute changes to existing accounts. Changes to accounts may be requested via e-mail, footprints or an Account Request form from the requester, authorized by

the Data Owner and sent to the OCCS Accounts Manager. The Account Manager makes the authorized changes and informs the requester when the changes have been made.

Management Access to Employees Accounts –
From time to time management may need access to e-Mail or files in employee's accounts that they would not normally have access to. Access will be granted for a supervisor to have access to an employee's accounts if that request is approved by at least one level of management above the person requesting the access. When such access is granted, the employee is to be notified if they are still an active employee.

Termination of Accounts –

Accounts and/or access is to be terminated when that account/access is no longer required to perform one's role at the University.

Student Accounts –
Students may keep their accounts for approximately twelve (12) months after their last enrolled semester. After that period, the accounts are scheduled for deletion. The students are notified via e-mail before termination to allow them time for exceptions and/or data migration. The decision to extend the account is at the sole discretion of the OCCS Account Manager.

Faculty/Staff Accounts –
The Universal Account Request form carries this statement in the Budget Unit Director's signature block:

> *"I approve the requested access for this employee and understand it is my responsibility to have this account terminated when the applicant's employment is terminated or job function no longer requires access to these systems."*

Account termination notifications from Budget Unit Directors are acted upon by the Account Manager at the time of receipt or the date indicated in the notification. The Budget Unit Director or Data Owner may request the termination of the account/access at any time, not just at employee termination.

The Human Resources department sends the Account Manager a list of employee terminations on a bi weekly basis. The Account Manager reviews the list and confirms with the Budget Unit Directors the desire to terminate the accounts and it's contents. Upon confirmation, the accounts are deleted or disabled and scheduled for future deletion using the expiration date given to the Accounts Manager.

Restoration of Accounts –

After an account has been deleted, there may reasons to restore the account at a later time. Restorations are handled as new account creations and require the same documentation and approvals. Deleted data may be restored upon documented approval from the terminating data owner.

Vendor Account Management –

Vendors are a vital part of the IT support function. There are two primary ways of providing access for vendors to provide service to the University. Either an individual account is created through the use of an Account Request form or the vendor makes use of a 'sponsored' account.

Sponsored Vendor Accounts –
Accounts may be created and assigned to a System Owner, Data Owner or System Administrator for the purpose of providing support services. The passwords for these accounts are managed by the sponsoring person. They change the password to the account and provide it to the vendor for the duration of the support event only. After the support event is over, the password is changed back to something known only to the account sponsor or the account is disabled. Sponsored accounts are not to be integrated with or match the sponsor's password. The account sponsor is expected to retain records on account usage. It is the responsibility of the sponsor to provide the vendor with a copy of

the Acceptable Usage Policy and the General & Employee MIDAS security awareness training content.

Emergency and Temporary Accounts –

To meet the needs of an emergency, a System Administrator or application administrator may create an emergency/temporary account to be used for the duration of the emergency only. The account creation and justification must be documented and submitted to the University Information Security Officer (ISO) within 48 hours of account creation. The ISO must be notified in writing/E-Mail when the account has been deleted. If the account is needed for more than 30 days, a formal Account Request form will be processed for the account.

Locking / Disabling of Accounts –

When the MIDAS password expires, MIDAS disables all MIDAS enabled accounts associated with the user by scrambling the password to something unknown to the user. The only way to have access to those applications again is to log into MIDAS and change the MIDAS password. If the MIDAS account (or any associated accounts) have been locked, then the user will be unable to access those accounts. Through Accounts tracking the Accounts Manager can disable all or just selected accounts as needed.

Banner Accounts –
Banner accounts are in a dormant (unusable) state after 120 days of non-use. Once a banner accounts becomes dormant, the existing password is disabled. They can be reactivated by getting a new banner password.

Suspension of Accounts –
User accounts may be suspended by the Security Staff if the account is involved in an incident. All or select services may be suspended depending on the scope of the incident. Suspensions will only be lifted with the approval of the Security Staff. Accounts marked in Accounts Tracking with the 'SUSP' status have been suspended in this fashion.

Quality Controls / Audits –

There are several quality controls in place to ensure that accounts are properly established and maintained and that only authorized accounts are created.

Simple Internal Accounts –
MIDAS connectors verify the account state before updating Accounts Tracking to validate that the intended actions were performed accurately and completely. Accounts are automatically repeatedly processed until the intended state is met.

Daily Checks –
Reports run daily on any access changes made to Banner accounts. These reports are sent via e-mail to the ISO, the backup ISO and the Accounts Manager. The ISO reviews these reports to verify that only approved changes were made and investigates any unusual entries from the report.

Monthly Checks –
Every month the Data Owners are e-mailed a report of all Banner Access changes made during the previous month. The Data Owners are to review this report and compare it to the changes that they have approved over that same time period. Any discrepancies are to be brought to the attention of the ISO.

Banner Budget Unit Director Audits –
At least annually, the Budget Unit Directors are provided a report of all of the people in their area that have Banner access, and what access rights they have. The Budget Unit Directors are given a

specific date to have reviewed the reports, marked any changes needed and return it to the Account Manager for processing. The details of this process can be found in the Budget Unit Director Banner Audit Procedure.

Banner Data Owner Audits –
At least annually and after the Budget Unit Director Banner Audit is complete, the Data Owners are provided a report of all of the people that have access to their Banner application(s), and what access rights they have. The Data Owners are given a specific date to have reviewed the reports, marked any changes needed and return it to the Account Manager for processing. The details of this process can be found in the Data Owner Banner Audit Procedure.

Account Management Exceptions -

Exceptions to the normal Account Management processes are handled on a case by case basis and must be approved by the University Information Security Officer.

Example of exceptions include:

- Lab accounts with multiple logins enabled – These are accounts that may be logged into a group of workstations by the account holder and used to run a specific application. This, in affect, turns the lab workstation into a kiosk.
- Shared accounts with a secondary process of auditing – This is an account that will be distributed to a number of individuals with a separate record of who has the account and where it was used. These accounts are typically limited to a particular network or are otherwise restricted.
- Non-Standard MIDAS Account IDs – These are MIDAS IDs that are not automatically generated. The request may be made through the Accounts Manager but must be approved by the ISO.
- Multiple Banner Accounts - Due to form permission difficulties or limitations, multiple Banner accounts may be issued to the same individual in rare instances.
- External Integrated Accounts - where a setup is done on the constituent system that are not controlled via MIDAS.

Definitions

Information Technology Resources are defined as computers, telecommunication equipment, networks, automated data processing, databases, the Internet, printing, management information systems, and related information, equipment, goods, and services.

OCCS is the acronym for the official name of the Office of Computing and Communications Services.

User includes anyone who accesses and uses the Old Dominion University information technology resources.

Policy References **ODU faculty, staff and students are bound by all applicable laws, policies, standards and procedures and guidelines. For reference, some frequently referenced documents are noted. This is a non-inclusive list and not intended to limit applicability of any other law or policy.**	
Ⓟ Policy Foundation:	Federal and State Law Policy 3505 Security Policy COV ITRM standard SEC501-01
Related Standards:	

Related Procedures, Forms:	Universal Account Request Form
Related Guidelines:	None
Maintenance:	Office of Computing and Communications Services
Effective Date:	Reviewed on an annual basis
Approved by: Pending	Rusty Waterfield Acting Assistant Vice President, Office of Computing and Communications Services