



OIT 61.001: Account Management – Obtaining Access To Enterprise Information Systems

Responsible Executive : Chief Information Officer (CIO)
Responsible Office: Office of Information Technology
Related Policy: UP 60.201
Approved-On Date: May 9, 2006
Effective Date: April 21, 2006
Revision Date: May 11, 2010

Policy

Current faculty, staff, students and authorized 3rd parties may request that an account be created for the purpose of accessing administrative systems. This account is issued by the Office of Information Technology (OIT)-EIS and is considered to be the property of Norfolk State University (NSU). The account is no longer valid once the association with the university is terminated. Access to the account may be revoked by the university at any time. In accordance to the COV ITRM Standard SEC501, no account will be provisioned until all required forms are fully processed, requirement for a successful background check has been verified, and required information security awareness training is complete.

Purpose

The purpose of this policy is to provide guidelines for access to the protected technologies such as Integrated Financial and Administrative Solutions (IFAS), Colleague, SpartanShield and any other systems supported by OIT-EIS. By signing the Information Security Access Agreement form, you agree to abide by the policies established by OIT in the use of this account.

Procedures for Accessing Specific Administrative Systems

IFAS

Official university accounts are available for faculty, staff and authorized 3rd parties as needed. Access to information contained within the system is granted on a “need to know” basis. All passwords for accessing university information systems must be kept confidential and used according to university policy. The steps for obtaining an IFAS account are outlined below.

1. The requestor will submit an IFAS Access Request Form to the IFAS Security Administrator. Also if the user will be performing departmental purchasing duties an Online Signature Authorization Form must be submitted as well.

2. If the requestor is a new user, the requestor must also complete and submit an **Office of Information Technology Request Form (ITRF)** to OIT Client Services to establish a network account. Upon creating the new user's network account, OIT Client Services will forward the ITRF form to the IFAS Security Administrator.
3. The IFAS Security Administrator will then establish the user's ID and temporary password in SYSADMIN and the corresponding application security per the signed IFAS Access Request Form. Using the Nucleus Security module (NUUPUS), a security class containing job running capabilities will be assigned to the user. An existing security class may be used or a new security class will be established, where necessary.
4. The IFAS Security Administrator will then provide to the user their IFAS user ID and temporary password. The information is delivered to the user in a secure manner in accordance with University and VITA current best practices. The user is also given information regarding IFAS training in this correspondence.

Colleague

Official university accounts are available for faculty, staff and authorized 3rd parties as needed. Access to information contained within the system is granted on a "need to know" basis. All passwords for accessing university information systems must be kept confidential and used according to university policy. The steps for obtaining a Colleague account are outlined below.

1. The requestor will submit a Colleague Access Request Form to the Colleague Security Administrator. In addition, if the requestor is a new user, the requestor must also complete and submit an **Office of Information Technology Request Form (ITRF)** to OIT Client Services for processing. Upon creating the new user's network account, OIT Client Services will forward the ITRF form to the Colleague Security Administrator.
2. The Colleague Security Administrator will establish the user's ID and temporary password in SYSADMIN, and in Colleague using the SOD and SVM screens, per the signed Colleague Access Request Form. If the user's parameters have not been previously established, a new security class will be created by the Colleague Security Administrator using the SCD screen in Colleague.

SOD	System Operator Definition
SVM	Staff/Volunteer Maintenance
SCD	Security Class Definition

3. The Colleague Security Administrator will then provide to the user their Colleague user ID and temporary password. The information is delivered to the user in a secure manner in accordance with University and VITA current practices. The user is also given information regarding Colleague training in this correspondence.

SpartanShield

Official university accounts are available for students, faculty and staff as needed. All passwords for accessing university information systems must be kept confidential and used according to university policy. The steps for obtaining a SpartanShield account are outlined below.

1. OIT-EIS on an ongoing basis in batch mode creates new SpartanShield accounts for currently enrolled students. Once the account has been established, the user may access SpartanShield and follow the “I’m new to SpartanShield” workflow which will guide them through the process in requesting their password. Once requested, the password is delivered to the user in a secure manner in accordance with University and VITA current practices.
2. Students who do not have a SpartanShield account but desire to obtain one may contact OIT Client Services and verbally request that a new account be created for them. OIT Client Services then notifies the OIT-EIS SpartanShield Support Team. A representative of the team verifies eligibility, contacts the requestor and asks a series of questions to verify identity. Once identity has been verified, the team representative creates a new account via Colleague (ST DRUS - DMI Registry User Set Up) or SA Valet and informs the requestor of their new SpartanShield user ID. The user may now follow the “I’m new to SpartanShield” workflow as mentioned in step 1 to obtain their password.
3. Faculty and staff who do not have a SpartanShield account but desire to obtain one may complete and submit an **Office of Information Technology Request Form (ITRF)** to OIT Client Services requesting that a new account be created for them. OIT Client Services then notifies the OIT-EIS SpartanShield Support Team. A representative of the team creates a new account via Colleague (ST DRUS - DMI Registry User Set Up) or SA Valet and informs the requestor of their new SpartanShield user ID. The user may now follow the “I’m new to SpartanShield” workflow as mentioned in step 1 to obtain their password.