Network Services Account Request

NOTE: The website URL for Workday reference guides that are referenced in this section is: https://jira.esg.wsu.edu/plugins/servlet/desk/portal/91

ASSIGNMENT

Complete a Network Services Account Request to request a Network ID or an AIS User ID (for view only access to Administrative Information Systems (AIS)). Instructions are provided in this section.

NETWORK ID

A Network ID (NID) is a unique identifier that provides access to computing and network resources at WSU.

Information Technology Services (ITS) requests that WSU faculty, staff, and students use the following self-service websites to create Network IDs and/or update Network ID passwords:

- its.wsu.edu/csd/ (to request a Network ID)
- login.wsu.edu (to update Network ID passwords)

The Network ID identifies the individual to University network services.

Assignment of a Network ID does not in itself provide access to University computer systems. A user must request specific authorization to access each system required.

AIS USER ID

AIS (Administrative Information Systems) view only access may be granted after an exception review. To request access to AIS, the user must:

- Contact the Crimson Service Desk by telephone 509-335-4357, or e-mail crimsonservicedesk@wsu.edu; and
- Complete and submit a Network Services Account Request.

An AIS User ID is an account assigned to an individual. The account allows the user to gain access to AIS.

NOTE: Assignment of an AIS User ID does not in itself provide access to computer information systems. The employee must request specific authorization to access each AIS application. Access to AIS is granted on a need-to-know basis. (See BPPM 85.33 for access authorization procedures.)
Network Services Account Request

**FORM INSTRUCTIONS**

Complete a *Network Services Account Request* to obtain, change, or delete one or more accounts per individual.

**Completing the Form**

Most sections of the form are self-explanatory.

**WSU ID Number**

Completion of **WSU ID Number** is required before the request may be processed.

**Affiliates**

The University assigns WSU ID Numbers to qualified affiliates requesting Network IDs.

**New Employees**

A new employee is assigned a WSU ID Number when Human Resource Services processes the applicable Workday Staffing business processes. (See the applicable Workday reference guides for instructions.)

**Changes**

For changes to a Network ID, see [Exception to Policy](#).

**Terminations**

Network IDs are permanent and are not terminated.

**Authorization**

Each request for an affiliate Network ID must be signed in ink by a University employee holding expenditure authority for the sponsoring department.

**Exception to Policy**

Network IDs are considered permanent and are changed under certain circumstances only; for example:

- Name changes
- Poor initial selection of Network ID
- Personal privacy issues

To request changes to a Network ID, complete the applicable fields in the Exception to Policy section near the bottom of the form. Alternatively, users may also call the Crimson Service Desk at 509-335-4357 during business hours.

Enter the current Network ID under **From** in the **Complete if changing Network ID** line.

**Routing**

Send the completed and approved form to Crimson Service Desk, mail code 1222.
Network Services Account Request

Security Administrator
ITS completes the requested action and notifies the requesting individual by interdepartmental mail, or by telephone if requested.

SECURITY
The security of network and computer services is partially dependent upon the actions of individual users. Each individual user is responsible for the following:

- Safeguarding the Network ID and password.
- Retaining the Network Services Account Request in a secure location.
- Not sharing the Network ID with others. ITS assigns a Network ID to an individual user.
- Immediately contacting the ITS Security Office if the confidentiality of a Network ID is compromised by telephone 509-335-4357, or e-mail abuse@wsu.edu.
- Not including any password in automated or preprogrammed logon procedures. The user must manually enter the password to gain access to online services.