Network User Id Policy

Summary

Authentication, in the form of a user ID and password, is a means of protecting CSU information assets from misuse or compromise and is required to access all University owned computers. After logging into the network with either the Novell NetWare or ProSoft Client (wired) or Odyssey Client (wireless), the user has access to the Windows desktop and/or network resources. Authorized users of the CSU network include currently enrolled students, faculty, staff, and allowed guests.

Purpose

The purpose of this policy is to set forth principles, procedures, and responsibilities for the creation, use, and maintenance of network user IDs.

Policy

- All users must have their identity verified with a unique network user-ID and password prior to gaining access to the Columbus State University network.
- CSU grants all faculty, staff, and currently enrolled students this privilege after they sign an agreement containing confidentiality, information security, and acceptable use information.
- Network user IDs consist of the user's legal name in lastname_firstname format. In the case where two or more users have the same name, the system adds a number to the user ID.
- Network user IDs cannot be changed unless there is a legal name change.
- Network user IDs of those users no longer enrolled or employed must be promptly disabled and/or removed from the database.
- Generic network user IDs may be issued under specific circumstances, such as for shared machines in departmental areas, and require the approval of the Director of UITS. Generic IDs are restricted to a specific workstation.
- Non-student network user IDs may be issued under specific circumstances, such as for a previously enrolled student to finish coursework.
- Users must comply with all University policies and local, state, and federal information security laws in order to maintain continued use of their ID.

Procedures and Responsibilities

- The systems administrator creates student user IDs at the beginning of each semester. The Banner Student Information System provides eligibility and enrollment status.

- The systems administrator creates faculty user IDs upon request. The Vice President for Academic Affairs (VPAA) office is responsible for submitting New User Account Request forms for faculty members.
- The systems administrator creates staff network user IDs upon request. The Human Resources (HR) office is responsible for submitting New User Account Request forms for staff members.

- The systems administrator creates generic user IDs upon request. Vice Presidents, Deans, Associate Deans, Department Chairs and Directors may request a generic ID via eQuest. Use of the generic ID is the responsibility of the requestor.
- The systems administrator creates non-student IDs upon request. Persons not currently affiliated with CSU, but with an academic purpose, may request a user ID from the VP for Academic Affairs.
- The systems administrator disables and/or removes student user IDs at the beginning of the first semester that they do not re-enroll. Faculty and staff IDs will be disabled and/or removed upon notice from HR.
- Users whose legal name changes may request a network user ID name change by contacting HR and submitting a request via eQuest. The systems administrator will make the change after verifying that Human Resources and/or the Registrar's office have processed the name change.

Student policy violations are handled as follows:

- The systems administrator will verify that a violation did indeed occur.
- The systems administrator will disable the violator's network user ID, make a notation in the user database, and notify the office of the Dean of Students.
- The systems administrator will reinstate the violator's privileges only upon directive from the VPAA's office.

- Faculty and staff violations are handled on a case-by-case basis with the involvement of the Information Security Officer, the Director of UITS, Director of HR, University Police (if necessary) and the violator's supervisor.
- End-users are responsible for the appropriate use of their network user ID.
- Systems administrators are responsible for the creation, maintenance, and removal of network user IDs as well as the availability, integrity, and confidentiality of the user database.
- Human Resources and the VPAA's office are responsible for keeping systems administrators informed of personnel changes.

Related USG Policy

5.11 (IT Handbook) Minimum Security Standards for USG Networked Devices & 5.12 (IT Handbook) Password Security

Last Update

4/17/2014

Responsible Authority

Chief Information Security Officer