Information Systems Security

FT_IT_UT_30

Responsible Officer
Rick Snider
Responsible Office
IT
Last Revision
2019-12
Re-evaluation Date
2021

Policy Statement

Consistent standards for network access and authentication are critical to the company's information security and are often required by regulations or third-party agreements. Any user accessing the company's computer systems has the ability to affect the security of all users of the network. Access to CU computer systems requires a CU-assigned computer account and password.

Rationale

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the corporate network are authenticated in an appropriate manner, in compliance with CU standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

Policy Procedures

New Employees

New employees are granted a network account once approval is granted from the Business Office. Shared drive access is granted per the direction of the appropriate departmental head, CIO, or cabinet member.

Employee and Student System Access

Information System access is managed using a CU-assigned username (or email address) and password. Employees are prohibited from sharing their access credentials. If there is an indication the credentials have been compromised, it is the employee’s responsibility to contact the IT department immediately.

Locking of Accounts

Repeated login failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the university locks a user's account after 5 unsuccessful logins on a domain-managed computer. Unlocking the account will require action by the IT department.

Screensavers

Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason screensaver passwords are required to be activated after 15 minutes of inactivity.

Remote Network Access

Remote access to the CU network via VPN or Splashtop is granted upon request. Security requirements and restrictions remain the same whether on-campus or when accessing the network remotely.

Computer Security

Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, users must strictly adhere to CU standards with regard to antivirus software and patch levels on their machines. Users must not be permitted network access if these standards are not met. All computers, whether CU-owned or personally owned, must have current anti-virus software installed.

Employee Termination

Employee network account are to be terminated when the employee clears the Business Office. Upon request by the appropriate department head or cabinet member, network and email access may be continued for a period of 30 days after the termination of employment.