PURPOSE

The principle of access control is to limit access to information based on a ‘need to know’. Access control is one of the keys to information security, this principal is violated when users, who do not or no longer have a legitimate ‘need to know’, retain access privileges. This violation is most frequently observed when users terminate their relationship with the University or transfer to a job with different duties and responsibilities. It is critical that access privileges be revoked, in a timely manner, when access is no longer needed.

SCOPE

This policy applies to all members of the Creighton University community (staff, faculty, students, contractors, consultants, temporaries, visitors, etc.) while using Creighton’s computing or networking resources. All users are expected to be familiar with and comply with this policy.

POLICY

Access privileges must be revoked in a timely manner when a user no longer has a need for such access.

DEFINITIONS

None

RESPONSIBILITIES

Supervisors are responsible for notifying the Human Resource Department when an employee terminates employment or transfers to a new position with new duties and responsibilities.

Human Resource Department is responsible for providing IT and others with access control responsibilities with timely reports of terminations and transfers.

Access Control Administrators are responsible for revoking the access of users who no longer have a need for access.

Information Security is responsible for maintaining and enforcing the policy.

ADMINISTRATION AND INTERPRETATIONS

This policy shall be administered by Information Security. Questions regarding this policy should be directed to the Information Security Officer.
### AMENDMENT/TERMINATION OF THIS POLICY

The University reserves the right to modify, amend or terminate this policy at any time. This policy does not constitute a contract between the University and its faculty or employees.

### REFERENCES TO APPLICABLE STANDARDS

- Information Security Philosophy
- Information Security Governance Policy
- Information Security Exception Policy
- Termination of Access Standards

### EXCEPTIONS

Requests for an exception to this Policy must be submitted via the Policy Exception Request Form. All exception requests will be handled in accordance with the Information Security Exception Policy and Standard.

### VIOLATIONS/ENFORCEMENT

Any known violations of this policy should be reported to the University's Information Security Officer at 402-280-2386 or via e-mail to infosec@creighton.edu.

Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with University procedures.

The University may advise law enforcement agencies when a criminal offense may have been committed.