PURPOSE

From time to time, situations arise that cannot be effectively addressed within the constraints of existing Information Security policies and standards. Nevertheless, Creighton’s security needs must not be compromised. To provide for “a standard way of doing non-standard things”, Information Security must provide a process for reviewing and approving or denying requests for exceptions.

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

Deviations from Information Security policies and standards shall not be permitted without approval via an authorized exception review process conducted by the Information Security Officer.

Evaluations of exception requests will take into account the compensating benefits to Creighton in each exception request. Requests that create significant risks without compensating controls will not be approved.

DEFINITIONS

None.

RESPONSIBILITIES

Information Custodians are responsible for requesting an exception of Policies and Standards that cannot be achieved.

Information Security Officer is responsible for conducting policy exception reviews as needed.

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

Internal Use Only
DRAFT
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 Standard

EXCEPTIONS

None.

APPEALS

Appeals to decisions reached through the exception review process will be heard by the Information Security Steering Committee. To register an appeal, please contact the chair of the Information Security Steering Committee.