

IT Security

Information Technology Systems and Services

IT Security Policy Review Process for UND

IT security policies and guidelines are implemented at UND in the interests of the entire community – to communicate to all users the kinds of actions that can help or hinder the availability and reliability of IT resources supporting UND's academic mission.

To ensure that UND's IT security policies and guidelines are fair and reasonable for all students, faculty, and staff, the following review process has been put in place:

1. *Development*

A notice will be posted on the [IT Security Policy web site](#) to communicate that a policy or guideline will be created on a particular topic.

For each proposed policy, the ITSO will assemble a group of Subject Matter Experts (SMEs). This group will meet face-to-face as needed, but development will primarily be done through correspondence. This group will have the following responsibilities:

- Identify the key issues and what to include in the policy/guideline.
- Determine what is most appropriate for the particular issue: a policy or a guideline.
- Collaborate to draft the language of the document.

The draft document will be sent to a specific group of campus individuals for a two week review period to solicit comments. This list will include (but is not limited to):

- UITC
- Office of General Counsel
- Audit Office
- Campus IT Managers/System Administrators
- Office of Student Government
- Dean's Council
- Loss Control Security Subcommittee
- University Senate
- Staff Senate
- Association of Residence Halls
- University Apartments Advisory Council

The ITSO and SMEs will review any comments and, if necessary, modify the draft document.

A copy of the draft document will then be posted on the [IT Security Policy web site](#) for one month for all members of the UND community to provide comments.

If comments are not received within the above timeframes, acceptance will be assumed.

The ITSO and SMEs will review any additional comments and prepare a "final" draft document.

2. *Publishing*

The IT Security Officer will present the "final" draft document to the University Information Technology Council (UITC) for their input and recommendations. According to UITC recommendations, a policy will be submitted to UND's President and cabinet for approval. Guidelines recommended by the UITC will be released immediately to the campus community.

3. *Education and Awareness*

The IT Security Officer will be responsible for distributing the new policy or guideline through a developed education and awareness program.

Policies and guidelines will be available on the [IT Security Policy web site](#) and will be identified as "in development", "draft", "published", and "under review".

4. *Measuring Effectiveness and Adherence*

The IT Security Officer and SMEs will be responsible for setting a review date of each policy/guideline based on the sensitivity and changing nature of the issue. The ITSO will post the review schedule for each policy and guideline on the [IT Security Policy web site](#).

The IT Security Officer will develop metrics (i.e., incidents, number of compromised systems, periodic audits, etc.) to measure the effectiveness of each policy/guidance.

The IT Security Officer will develop procedures to periodically audit compliance to existing policy/guidance documents.