Introduction
Information Technology
Security Guidelines
NSHE Security Interest Group

Overview
The NSHE SIG guidelines are intended to assist member institutions with the application of current NSHE program policy. The guidelines are not policies in themselves; they are recommendations concerning the application of technical and other controls.

Effective security is a team effort involving the participation and support of all member institutions. All NSHE employees, students, and institutional affiliates have the potential to negatively affect the security, functionality and integrity of NSHE computing and network resources. These guideline documents can define shared goals and guide in the efficient application of limited technical/security staff time and resources. The SIG intends that these guidelines will result in improved levels of security and efficiency for all NSHE institutions.

Scope
These guidelines are intended to be consistent with existing NSHE system-wide program policy. Institutions should use these general guidelines to assist in the production of baselines, minimum standards, documentation, training plans, checklists, and procedures tailored to the needs of the individual institutions.

These guidelines should apply to all employees, students, guests, visitors, consultants, temporaries, and other workers at the member institutions, including all personnel affiliated with third parties (e.g., contractors and subcontractors). These recommendations also apply to all equipment used by NSHE or NSHE member institutions, and apply to any equipment connected to an NSHE network. Certain sensitive or critical systems may be covered by program-specific or system-specific policies and procedures, may be affected by contractual obligations, or may be covered by state or federal legislation that mandates stricter or more extensive controls than are detailed in these guidelines.

Audience
The bulk of the recommendations in these guidelines are directed at institutional information security staff, and system and network administrators. The guidelines also contain recommendations for end-users.

Related Documents
See the NSHE Computing Resource Policy and the NevadaNet policies for details on appropriate usage of computing equipment and NSHE networks. Also see the appropriate related institutional policies and procedures.

Exceptions
For technical or other reasons, institutions may support systems or networks that substantially deviate from best practice. Institutions should develop documented procedures for reviewing, documenting, and managing these situations.

Training and Security Awareness
Institutions should develop communication, training, and security awareness programs or procedures tailored to their needs and constituencies. For example, staff members who have privileged system access or who have access to sensitive or confidential information should be reminded of their responsibilities regarding the special access they have. All account holders and NevadaNet users should be aware of NSHE and NevadaNet policy and of their responsibilities as end users.

Review
These guidelines are written and approved by members of the NSHE Security Interest Group. The guidelines strongly reflect industry best practice and also reflect a strong consensus among the NSHE SIG group members.

Teams of volunteers from the NSHE Security Interest Group write these guidelines. Each team consists of, at a minimum, a lead author, an editor, and at least one technical reviewer. Once the team has composed a draft, the team forwards it to the SIG for review and revision.

Endorsement
Each institutional Chief Technical Officer will designate a representative to review and endorse the guidelines. These representatives vote on the guidelines via email. Voting is on a simple majority system. Once approved by the institutional representatives, the guidelines will then go to the Chief Technical Officers for final endorsement.

The guideline drafting process may be altered by consensus of the SIG members or by the SCS System Security Officer. The endorsement process may be amended by the SIG in conjunction with the institutional Chief Technical Officers and/or the System Security Officer.