Access and Authentication Guidelines
For Information Resources
NSHE Security Interest Group

Scope

These guidelines are a series of recommended general best practices pertaining to network and resource access, authentication, and logging.

We encourage campuses to survey their information and infrastructure assets. A thorough understanding of the degree of sensitivity of data or resources can guide the selection of appropriate security controls to protect those assets. More critical resources require more extensive protection; simpler scenarios may be acceptable for less critical resources. For example, a multilevel authentication scheme with detailed logging may be a good choice for protecting certain financial or medical information, but a very simple, easy-to-use authentication method may be acceptable for a student lab.

End-User Passwords and Account Security

1. Authorized users are responsible for the security of their accounts and passwords. Account credentials may not be shared with anyone, including family members and trusted associates. Account holders should keep passwords secure; users should not write down passwords, should not e-mail passwords, and should not store passwords in a means readily accessible by other users. Account holders may be held liable for any inappropriate activity tied to their accounts, such as copyright violations or other illegal activity, exposure of confidential or proprietary information, or harassment of other users.
2. Because information contained on portable devices is especially vulnerable, special care should be exercised; this could include the use of passwords and the encryption of data.

Guidelines for Device/System Configuration and System Administration

1. System-level passwords and passwords for privileged access should be changed on a regular basis; where practical, systems should be configured to enforce expiration periods for passwords.
2. When possible, software should be configured to enforce passwords of reasonable complexity and an appropriate minimum length, while maintaining a realistic ease of use.
3. Account sharing is discouraged. Where shared accounts are necessary for technical or logistical reasons, passwords should be changed regularly. Resource access for the shared account should be limited to strictly what is necessary. For example, a shared account password should be changed when a user who knows the password no longer requires access.
4. Student computing labs should require authentication in order to manage access to copyrighted materials, licensed software, and for potential legal reasons, e.g. minors participating in a campus program.

Review and Removal of Accounts and Related Access

When possible, account creation, deactivation, and removal should be automated and synchronized with information from enrollment and/or employment systems.

Institutions should generate documented procedures for the creation, removal, activation or deactivation, and any other processes involved with accounts.

Authentication Logs

Logging levels should be commensurate with the sensitivity of the resource to be accessed. For most resources and systems, this entails logging both successful and unsuccessful authentication attempts. Where DHCP is used, logging should allow the association of an IP assignment with the corresponding user. Campuses should create log review and retention procedures. Member institutions should be aware of the laws and policies that may affect their own campuses, departments, and programs (i.e., HIPAA, Sarbanes-Oxley, etc.).

Remote Access and Authentication

Remote (off-campus) access to resources should be formalized and managed per campus or institution. Access should be restricted to secured protocols (i.e., those that encrypt their traffic--SSH, POP3 secure, IMAP secure, etc.). Where authentication credentials must pass over possibly-insecure network segments, we recommend the use of highly secure protocols, such as NTLM v2, Kerberos, or LDAP over SSL. Where practical, legacy or unencrypted authentication protocols should be disabled on both clients and servers.

Guest Accounts and Temporary Access

When campus guests require network or system access, their needs should be met with temporary guest accounts with limited resource access. Account activity should be regulated, and these guest accounts should be managed according to established procedures. Institutions must be aware of licensing implications of guest accounts with respect to systems, devices, software, and information services.

Centralized Authentication

Campuses are encouraged to develop centralized authentication systems.
When appropriately planned and implemented, centralized systems can provide better services to users, reduce support costs, and improve security. Systems administrators, software developers, and data stewards should make use of centralized authentication system where it is possible and prudent to do so.

Recommendations for a centralized authentication system include secure data transmission, cross-platform compatibility, and the use of standards (i.e., LDAP, Kerberos, etc.). Automation is highly recommended in order to create, expire, and delete accounts. The system should also provide the ability to manually create accounts for the exceptions, and incorporate tools for managing the exceptions.

Review and Approval

Revision History