ADMINISTRATIVE POLICY

Password Policy

POLICY STATEMENT

Passwords are a critical part of information and network security. Passwords serve to protect user accounts, but a poorly chosen password, if compromised, could put the entire network at risk. As a result, all employees and students at Nevada State University (NS) are required to take appropriate steps to ensure that they create strong, secure passwords and keep them safeguarded at all times.

REASON FOR POLICY

The purpose of this policy is to set a standard for creating, protecting, and changing passwords such that they are strong, secure, and protected.

PROCEDURES

Password Construction Guidelines

Passwords are used to access any number of institutional systems, including workstations, the network, e-mail, and server-based applications. Poor or weak passwords are vulnerable to compromise and put the entire system at risk. Therefore, strong passwords are encouraged and enforced via system policy on systems with access to sensitive data.

1. Passwords should not be based on well-known or easily accessible personal information
2. Using a mix of alphanumeric and non-alphanumeric characters increases the strength of a password and is recommended

Password Protection Guidelines

1. Passwords should be treated as confidential information. No employee shall provide their password to another person including superiors, co-workers, friends, or family members.
2. Passwords should not be written down in an unsecured manner, such as paper, unless it is kept in a secured, lockable location
3. Refrain from using the “Remember Password” feature of applications on public or unprotected computers
4. Passwords used to gain access to campus systems should not be used as passwords to access non-work related accounts or information
5. If an employee either knows or suspects that his/her password has been compromised, it must be reported to Information & Technology Services (ITS) and the password changed immediately

Password Resets
It is necessary for the ITS Support Center to make positive identification of individuals requesting password resets to prevent electronic identity fraud. In order to achieve this, the following procedures are to be followed:

Employees

- Self-service solution: Use the NS Portal (http://my.nevadastate.edu) to reset forgotten passwords. Users must first enroll into the system to use this option and it is available 24x7.
- Support request: If contacting the ITS Support Center for a password reset employees will be required to verify the following information:
    - By phone:
        1. First and last name
        2. NSHE ID
        3. Date of birth
    - In person:
        1. Photo ID
    - By online ticket:
        1. Request must be submitted by the account holder

Students

- Self-service solution: Use the NS Portal (http://my.nevadastate.edu) to reset forgotten passwords. Users must first enroll into the system to use this option and it is available 24x7.
- Support request: If contacting the ITS Support Center for a password reset students will be required to verify the following information:
    - By phone:
        1. First and last name
        2. NSHE ID
        3. Date of birth
    - In person:
        1. Photo ID
    - By online ticket:
        1. Request must be submitted by the account holder

Group Accounts

- Group account password resets must come from the designated account manager, their designee, or the department head.
- Support request: If contacting the ITS Support Center for a password reset, group account holders will be required to verify the following information:
    - By phone:
        1. First and last name
        2. NSHE ID
        3. Date of birth
    - In person:
        1. Photo ID
    - By online ticket:
        1. Request must be submitted by the account manager, their designee, or the department head

Multifactor Authentication
Multifactor authentication (MFA) shall be utilized, where supported, for applications or systems that store, process, or transmit sensitive information. This includes, but is not limited to email, cloud storage, financial, human resource, and student information systems.

CONTACTS

SUBJECT	CONTACT	PHONE	EMAIL
Primary Contact(s)	Brian Chongtai	702-992-2410	brian.chongtai@nevadastate.edu

DEFINITIONS

Multifactor Authentication: A security process that requires user to provide two or more independent forms of verification to gain access to a system, application, or data. MFA significantly enhances security by reducing the risk of unauthorized access, even if one factor, such as a password, is compromised.

RELATED INFORMATION

HISTORY

Revised 8/5/24