2.1.2. Supervisors, administrators, or other University Community Members must not request or

4.3. The Information Security Services team will run periodic reviews to maintain the highest level of compliance and security without impeding business operations.

5. Violations and Enforcement

5.1. Enforcement may include removal of systems from the NAU network, removal of access privileges to NAU IT Resources, removal of Internet Connectivity, or removal of access to the NAU User Account.

Section II. Privileged Access

1. Definition and Description

1.1. Privileged Access, often referred to as "administrator," "admin," "root," or "service" accounts or access, exist in all operating systems, databases, and applications. Privileged Access is commonly used for running specific services or processes, which typically have elevated privileges that allow for modifications to the operation of an IT Resource, as well as full or elevated access to files, logs, and other user account privilege levels.

1.2. Due to the nature of the high level of access, Privilege Access accounts are targeted by attackers seeking to compromise and use them for unauthorized access. The compromise of a Privileged Access account poses significant risk and harm to the University, including data loss, creation of attacker-controlled accounts, and continued control of IT Resources.

2. Issuance and Management

2.1. A system administrator or designee must approve the granting of Privileged Access to systems or applications which they administer and for which they are responsible.

2.2. Privileged Access may be associated to a single individual, service, group, or team of individuals, and should remain active only while there is an identified business need for these access rights.

2.3. Privileged Access accounts should be reviewed periodically by the appropriate System Administrator, Data Steward, group owner, or supervisor. This review is required for systems where Sensitive or Highly Sensitive Data resides, is transmitted, or processed.

2.4. When a user with Privileged Access separates from the University, a System Administrator or designee must revoke that individual's Privileged Access to University IT Resources.

3. Responsibilities and Usage

3.1. All Privileged Access usage must be logged and monitored for anomalous activity. Anomalous activity associated with Privileged Access should be automatically alerted with notifications to the Information Security Services team and/or the IAM team.

3.2. Privileged Access must not be used for day-to-day operations or non-security functions that can be accomplished by a non-Privileged or elevated account including, but not limited to:

Browsing the web
Email, instant messaging, or other electronic communications
Opening of attachments

3.3. Privileged Access shall not be used for purposes beyond facilitating operations of the intended IT Resource and may be used to perform job duties including, but not limited to:

Installing, upgrading, or troubleshooting system or application software
Relocating an individual's files
Performing repairs necessary to return an IT Resource to normal operations
Running security programs
Managing system backups

Monitoring and fine-tuning an IT Resource to ensure continuity of operations, reliability, and security

3.4. Privileged or elevated access may be used to grant, deny, or change access or privileges to another individual for authorized account management actions. Examples include, but are not limited to:

Disabling or removing an account suspected of misuse or attempting to compromise privileged accounts, such as root or administrator
Disconnecting an IT Resource from the network when suspected compromise or security incident is reported
Accessing files for law enforcement authorities or other third parties with a valid subpoena