Plan 1 – University of North Florida (UNF) Information Security Plan

Institution: University of North Florida
URL: https://www.unf.edu/its/polproc/Information-Security-Plan.html UNF Home
Relevant for: Purpose, Scope, Roles and Responsibilities, Exceptions/Exemptions, Enforcement

Purpose

Defines the IT security standards and procedures to safeguard the confidentiality, integrity, and availability of all IT systems, data, and resources under UNF's Information Technology Services (ITS). It also ensures compliance with applicable laws, regulations, and internal policies. UNF Home

Scope

Applies to all information systems and resources connected to UNF's networks. It supplements ITS policies and aligns with federal, state, and institutional requirements. UNF Home

Roles and Responsibilities

The plan outlines duties for security roles such as the Security Manager and support offices. ITS leadership coordinates risk assessments, safeguards, monitoring, and program adjustments. UNF Home

Exceptions/Exemptions

UNF maintains a Security Exceptions standard where specific control exceptions can be approved by the Chief Information Security Officer (CISO) under documented conditions, with compensating controls where appropriate. UNF Home

Enforcement

Users and organizational units must adhere to security program requirements. Exceptions must be formally requested, justified, and documented per institutional processes. The plan references enforcement through ITS standards and compliance oversight (implied through the structure of the security program and associated standards). UNF Home

Plan 2 – Washington and Lee University Information Security Plan

Institution: Washington and Lee University
URL: https://my.wlu.edu/its/about-its/information-security-plan Washington and Lee University
Relevant for: Purpose, Scope, Roles and Responsibilities, Enforcement

Purpose

Supports the academic mission by ensuring confidentiality, integrity, and availability of IT assets in accordance with institutional policies, risk management plans, incident response procedures, and compliance tools. Washington and Lee University

Scope

Applies to any use of the University's computing or network resources as defined by relevant use and confidentiality policies. It covers systems managed by the ITS and may extend to third-party provided services. Washington and Lee University

Roles and Responsibilities

Defines specific roles such as Chief Information Security Officer (CISO), Data Trustees, and Incident Response Team members. The CISO coordinates security efforts, risk management, incident response, and security awareness activities. Washington and Lee University

Exceptions/Exemptions

While the main plan site does not list a dedicated exceptions subsection, the broader policy program includes governance and associated procedures (e.g., confidentiality, covered data definitions) that collectively influence allowable exceptions through policy context. Washington and Lee University

Enforcement

Security and compliance are maintained through proactive tools (antivirus, firewalls, network scanning) and formal incident response procedures. Enforcement is driven by ITS policies and supported by monitoring, scanning for vulnerabilities, and defined procedures for addressing weaknesses uncovered during proactive assessments. Washington and Lee University