

Policy Change Log - January 2022

Major Edits

Major edits include anything that alters the purpose or effect of the document.

Title
Vulnerability Management Standard for Information Technology
<p>This represents an overhaul of the current Vulnerability Management Standard, which will also supersede the Vulnerability Management Policy.</p> <p>Major shifts include:</p> <ul style="list-style-type: none">• Reducing the redundancy and potential differences between the SAI program documentation and processes, the Information Security Controls Standard, and this Standard with respect to timelines and classes of vulnerabilities. This revision will remove most of the detail that is redundant between those three sources of authority.• Providing clarity and guidance in areas where those have been requested, most notably for Cloud environments. This revision represents a step in organizational maturity with respect to cloud computing.• More clearly allocates responsibility to units and individuals for managing security vulnerability detection and remediation, and reinforces SAI registration and training requirements.• Taking a maturity step in application development vulnerability policy. This has been an ISO 27002 weakness for us, that this revision attempts to address.
103 - University of North Carolina at Chapel Hill Policy on Retention of Financial Records
Retired - The content of the policy is duplicated in another policy.
Vulnerability Management Policy for Information Technology
Retired - The content of the policy is being relocated to a University Standard or Procedure.