Informing the UNC-Chapel Hill community about changes to technology and privacy policies.
new policies

Enterprise Data Governance Policy

- Formerly the Institutional Data Governance policy
- Assigns stewardship responsibilities for the protection of Enterprise Data.
- Empowers and charges the Enterprise Data Coordinating Committee (EDCC) to guide University Constituents and recommend Standards and Procedures for Data management.
- Applies to University Constituents with responsibility for management of University Enterprise Data.

Enterprise Data Governance Standard

- Establishes and defines roles and responsibilities of EDCC and various Data management roles.
- Defines the various data types of Enterprise Data and identifies the Data Trustee responsible for each type.
- Applies to University Constituents with responsibility for management of Enterprise Data.
The following documents can be found on the ITS Policy Review Page. These will be available for comment through March 9th. https://its.unc.edu/its-policy-review/

**IT Change Management Policy**
- Aims to effectively and thoughtfully communicate proposed IT changes across the University and minimize possible negative impact to effected systems and users.
- Ensures that all required elements for a change are in place prior to implementation.
- Applies to University business units and constituent individuals responsible for material changes to Production IT systems, applications, and services.

**IT Change Management Standard**
- Sets minimum requirements and provides recommended steps for classification, implementation, and authorization of IT changes to provide a secure transition.
- Applies to University units and constituent individuals responsible for material changes to production IT systems and applications.
for review.

The following documents can be found on the ITS Policy Review Page. These will be available for comment through March 9th.
https://its.unc.edu/its-policy-review/

**IT Access Control Policy**

- Establishes access controls that provide security to University information by limiting exposure and system access.
- Lists the various aspects of Access Rights Management that require actions and process.
- Applies to University Constituents and units responsible for management of IT systems or University Enterprise Data.

**IT Access Control Standard**

- Requires that Constituents create and follow processes to regularly audit and review access to University systems.
- Applies to University Constituents and units responsible for management of IT systems or University Enterprise Data.
IT Vendor Management

- Drafts of a new IT Vendor Management Standard are under development. Expect to hear more as this moves forward. If you have a particular interest in this topic, feel free to contact the ITS Policy Office, and you may win an early review of the drafts, or other valuable prizes! (really just more opportunities to review drafts).
Sending Feedback

- The IT Policy Office continuously reviews and updates IT Policies to best serve the University's Information Technology needs. We are always soliciting feedback on new policies. All feedback received by the IT Policy Office is considered for the policy review process.
- If you have feedback on this bulletin, on IT policy development or management, or on any campus IT or privacy policy document, please feel free to contact Kim Stahl via the ITS policy staff email its_policy@unc.edu, or give us specific feedback on the ITS Policy Review page: https://its.unc.edu/its-policy-review/

ITS Policy Office
ITS Manning, Office 3008
Campus Box 3420
Chapel Hill, NC 27599-3420
919.962.3987
its_policy@unc.edu