Classifying Your Data

Andrew Yoder, Lead ECM Architect

Protected information should only be shared to meet a legitimate business need. The University provides tools specifically designed to help you share Princeton information safely.

Sharing Data

Restricted and Confidential information must be encrypted. It is recommended that unrestricted within Princeton and Public data is encrypted whenever possible.

What is considered to always be Restricted?

- Social Security Numbers
- Bank account numbers
- Driver's license numbers
- State identity card numbers
- Credit card numbers
- Protected health information (as defined by HIPAA)

Who can help me classify my data?

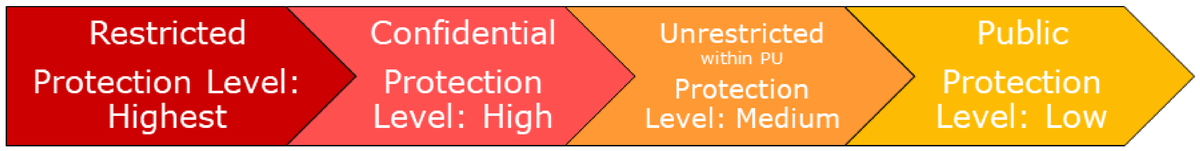
- Information Security Office
- Office of General Counsel

How do I know when I should not keep data?

The Records Management office can help to identify and implement a record retention schedule. It is important to make sure data is retained only for the appropriate lifecycle of that data. If data is past its operational, legal, or audit purpose it should be disposed of appropriately.

Everyone shares a responsibility to protect Princeton's information, whether you are the owner/steward of the information or need to access it.

- **Share Safely:** Information may only be shared or accessed in accordance with Princeton's Information Security Policy
- **Protect all information on all devices:** Recipients of University information must take appropriate measures to safeguard its confidentiality, no matter where it resides.
- **Report possible exposure:** Any unauthorized access to restricted information must be reported. If you suspect University information has been exposed, contact the Help Desk immediately at 258-HELP



Restricted Information

- Handle Restricted information with the greatest of care, and for legitimate business purposes only. Restricted information is afforded special protections in addition to the provisions within University policies, and is governed by state and federal law
- Only software approved by the Information Security Office may be used to store/share restricted data

Confidential Information

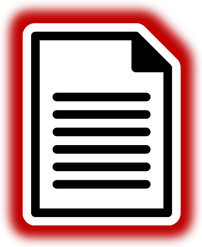
- Confidential information includes a range of data that requires safe handling and protection. It is not intended to be shared freely and you must take care to safeguard it

Unrestricted within Princeton

- Includes anything intended to be freely shared among members of the University community

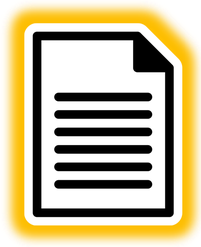
Public

- Information intended to be shared or disclosed inside or outside of the University

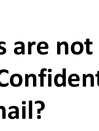


https://protectourinfo.princeton.edu/

https://records.princeton.edu/



https://informationsecurity.princeton.edu/



Did you know users are not permitted to share Restricted or Confidential data via e-mail?

Your Responsibilities

- Do not divulge, copy, release, sell, alter, or destroy information unless necessary
- Contact the Office of General Counsel prior to disclosure for legal purposes
- Contact the appropriate office prior to disclosure to regulatory agencies, inspectors, examiners, and/or auditors
- Understand the classifications and classify appropriately

Where Can I Store My Data?

Individual Use

- Google Drive*
- Microsoft Office 365 OneDrive for Business
- Dropbox for Princeton*

Departmental Use

- Central File Server
- Google Shared Drives*

Data for an Application

- Central File Server

Research Data

- Research Computing Storage Service

Collaborating with users outside of Princeton

- Google Drive*
- Dropbox for Princeton*

*Not approved for restricted data

https://princeton.edu/storage

PRINCETON UNIVERSITY