Campus Data Owners:
Best Practices in Protecting University Data

ODU Data Classifications

Highly Confidential
Unauthorized disclosure of highly confidential information can adversely or seriously affect the University as a whole or in part.

Protected
Unauthorized disclosure can adversely affect persons associated with the University, although it may not necessarily affect the University as an entity.

Public
Designed to be routinely disclosed and made freely available.

Identify
Identify where you have stored data under your control. In addition to your own workstation's hard drive, check to see if you have stored data on your departmental file server drives, your departmental or campus web servers, portable devices such as laptops or PDA's, and storage media (disks, USB keys, CD's, etc). Also identify where you have stored data on paper.

Understand
Each person is responsible for understanding the level of data they access and whether it can potentially cause the institution or individual harm. Make your determination based on the data classifications used by the University. Each person is responsible for the security of their computer accounts, passwords, and work stations.

Collect Wisely
Data should be collected only where that element is appropriate. Stop and think whenever you are handling Social Security numbers, credit card numbers, bank account numbers and access codes, driver's license numbers, and other sensitive personal information as part of your daily duties. Why do I have this data? Is it necessary for this transaction? If you do not absolutely need it to transact that business, dispose of it. Do not collect any other information that is not necessary for direct support of the current process. If the data isn't collected and stored, it cannot be compromised.

Store Securely
To store securely, you must know which storage location is to be used for what purpose. If collection of sensitive data is absolutely necessary, do with it what is necessary and then delete the files. Consult with your TSP to determine if you are protecting your data adequately. Never use personal storage mediums, such as flash drives, discs, or online storage options.

Dispose
Dispose means deletion from currently used drives (and then deleting your deleted items), securely wiping drives you no longer need, destroying storage media (disks, USB keys, CD's, etc.), and shredding paper.

Report
Maintain a professional environment where data abuse is not tolerated. Report suspected cases to the Information Security Officer at OCCS.

Office of Computing and Communications Services
Old Dominion University