



Take a second
to be secure.

The Security Minute

A communication of the Longwood University Information Security Office

Read *The Security Minute* Online: www.longwood.edu/infosec

September 2010

IN THIS ISSUE

DATA CLASSIFICATION
PART II

SECURITY SPOTLIGHT:
BE AWARE...

Security Spotlight:

**Be AWARE...
Don't SHARE!**

Longwood University uses the LancerNet ID and LancerNet Password to permit access to more than just email and office computers. By providing your LancerNet ID and Password to a colleague, or anyone for that matter, you have also potentially exposed all of the information you have access to through the myLongwood portal, including but not limited to your Payline Records, your Employee Benefit Records and anything you access in Banner.

Same goes for students. Sharing LancerNet IDs and LancerNet Passwords with an online grade-gambling site, exposes more than just grades. Registration and Student Account information are also kept in myLongwood.

Data Classification :: Keep—On

"Handling" information relates to when you view, update, delete, transfer, mail, store, or destroy data. It also relates to how you transfer the data from one location to another. Data is not always stored electronically. Occasionally it could be paper stored in a filing cabinet or in a binder. Additionally the data could be in a report or in a memo. Therefore, it is important you understand how to handle these situations based on the data's classification.

Based upon how data is classified (Public, Internal or Restricted), it may need precautions for handling. Here is an overview of the University developed standards for the **storage** of University data.

Recall **Public** data is information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data, while subject to University disclosure rules, is available to all members of the University community and to all individuals and entities external to the University community. Currently there are no standards for the storage of Public data based on the sheer nature of "open to the general public."

Internal data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Internal data is information that is restricted to members of the University

community who have a legitimate purpose for accessing such data.

The handling standards for Internal data stored in electronic format whether on a server, Desktop workstation, Laptop, USB drive, Handheld and the like require that the device simply be *University owned* and servers must *not be publically accessible*. For Internal data stored in non-electronic format whether paper documents, white board, photographs and the like require that the data be stored in a secure location with appropriate physical controls, typically determined by the data owner.

Restricted data is information protected by statutes, regulations, University policies or polices or contractual language. It may only be disclosed to individuals on a need-to-know basis. Therefore, the handling standards are, in addition to the standards for storing Internal data, stricter.

Storing Restricted data in electronic or non-electronic format requires the Data Owner's approval when stored on a Desktop workstation, Laptop, USB drive, Handheld and the like, as well as when storing Restricted data on paper, white boards, photographs and the like. Storing Restricted data in non-electronic format may also require labeling, per the Data Owner's discretion.

The security of all University owned data should be a high priority to any faculty or staff member at Longwood. Storing, transmitting and disposal of University data can cause said data to become vulnerable. It is up to each Longwood user to know, understand, and follow the policies and standards associated with the Universities Data Classification and Handling. The University's policy on Data Classification can be found online at:

www.longwood.edu/vpaffinal_policy_base/6000/6134.htm

and the associated standard for Data Handling can be found online at:

www.longwood.edu/infosec/data/DataHandlingStandards.htm



Keep—On is Part II of a multi-part series on Data Classification. Look for "Data Classification : Carry & Move—On" next month, with a continued recap of the Data Handling Standards found online at www.longwood.edu/infosec/data/DataHandlingStandards.htm



The Security Minute is a monthly publication aimed at raising awareness of information security related issues and concerns.

Please contact Jennifer Eckrote at 434-395-2034 or eckrotejl@longwood.edu.