Wake Forest University

Standard

Electronic Non-Public Information

Director of Information Security

Revision History

Revision	Date	Summary	Editor
1.0	November 19, 2012	Original release	Joel Garmon

Wake Forest University
Electronic Non-Public Information Standard

Introduction and Purpose

All WFU departments are responsible for establishing, monitoring and managing controls for electronic non-public information (e-NPI). Departments are also responsible for ensuring that individuals with access to e-NPI are trained and aware of their responsibility to protect e-NPI in accordance with University standards and requirements. Appropriate IT support personnel such as Information Systems, departmental IT staff or ITGs are responsible for implementing technical controls for e-NPI safekeeping in consultation and coordination with the responsible department.

Definitions

The Information Security Department is responsible across the University for all aspects of information and data security and complying with laws and regulations related to cyber security.

Information Systems (IS) Security is in the Information Systems Department and is responsible for all information and data security within IS. IS Security is also used as a resource for Information Security

Data Custodian -- Person or entity that can authorize or deny access to certain data, and is responsible for its accuracy, integrity, and timeliness.

Scope

This standard is applicable to all WFU departments, schools, and offices. This includes faculty, staff, and students contracted employees and temporary employees.

Standard

The following constitute e-NPI data elements as determined by WFU:

- Social Security Number
- Bank Account Information
- Credit or Debit Card Numbers and Account Information
- PINS/Passwords
- Employee Salary, Benefits, Disciplinary and Information
- Admissions Records
- Donor Records
- Research Records covered by Non-Disclosure Agreements
- Driver's License Numbers
- Government Issued Identification Numbers
- Passport/Alien Registration
- Personal Health Information
- Education Records
- Digital Signatures
- Biometric Data including fingerprints
- Any other numbers or information that can be used to access a person's personal financial resources.

Departments are required to designate individual(s) ("Data Custodians") who will be responsible for data protection in all of their departmental systems that store e-NPI. These Data Custodians will work with their appropriate IT support personnel to accomplish the following minimum requirements:

Access to e-NPI

- Business and technical processes for granting and removing access to e-NPI must be established.
- Access to e-NPI shall be provided only on a need to know basis and reasonable business practices must be implemented to protect the e-NPI.
- Employees granted access to e-NPI must immediately notify Information Security if they suspect a breach or loss of control over e-NPI. For example, contact Information Security if a laptop containing e-NPI is lost or stolen.

- Annual recertification of access to and the location of e-NPI data must be performed and documented by the Data Custodian. This entails re-validating all users and deleting data no longer required to support the department.

Sharing e-NPI

- e-NPI transfers and downloads, both internal and external to WFU, must be approved in advance and in writing by Information Security. For example, Information Security approval is required when creating a copy of e-NPI for internal use or when transferring e-NPI to a third party for any reason.
- If sharing of e-NPI is part of a project, the approval documentation must be part of the project plan.
- All documentation of Information Security approval will be retained by Information Security.

Storage of e-NPI

- e-NPI data must not be stored on laptops, CDs, flash drives, or other removable or mobile devices unless approved in advance and in writing by Information Security.
    a. Devices that are encrypted using Information Security approved methods are automatically approved for storage of e-NPI. See Appendix A for approved encrypted devices.
- Where cost effective, systems must be designed to log and audit access to e-NPI.
- Systems that store or process e-NPI must adhere to the current Information Security policies and standards. Copies of the most current policies can be accessed by using the following link; http://infosec.wfu.edu/standards/.

Destruction of e-NPI

- e-NPI shall be properly deleted or destroyed when the e-NPI is no longer needed for business or legal purposes.

Appendix A
Approved Encrypted Removable Media

Here is the list of devices that are approved for use with e-NPI.

Microsoft Bitlocker encrypted drives

Recommended Flash Drives.

Item	Model	Comments
Kingston DataTraveler Vault Privacy Edition USB Flash Drive – 2 GB	Mfg. Part#: DTVP/2GB UNSPSC: 43202005	Deacon Depot – Choose CDW or Office Max vendor sites.
Kingston DataTraveler Vault Privacy Edition USB Flash Drive – 4 GB	Mfg. Part#: DTVP/4GB UNSPSC: 43202005	Deacon Depot – Choose CDW or Office Max vendor sites.
Kingston DataTraveler Vault Privacy Edition USB Flash Drive - 8 GB	Mfg. Part#: DTVP/8GB UNSPSC: 43202005	Deacon Depot – Choose CDW or Office Max vendor sites.
Kingston DataTraveler Vault Privacy Edition USB Flash Drive – 16 GB	Mfg. Part#: DTVP/16GB UNSPSC: 43202005	Deacon Depot – Choose CDW or Office Max vendor sites.
Corsair USB 16GB Padlock Flash Drive	Mfg#: CR2-CMFPLA16GB Contract: Amerinet Tier 4 VH10213	Deacon Depot – Choose CDW or Office Max vendor sites.
Corsair USB 8GB Padlock Flash Drive	Mfg#: CR2-CMFPLA8GB Contract: Amerinet Tier 4 VH10213	Deacon Depot – Choose CDW or Office Max vendor sites.
Kanguru Defender Elite 1GB USB FD	Mfg#: KAR-KDFE-1G Contract: Amerinet Tier 4 VH10213	Deacon Depot – Choose CDW or Office Max vendor sites.
Kanguru Defender Elite 2GB USB FD	Mfg#: KAR-KDFE-2G Contract: Amerinet Tier 4 VH10213	Deacon Depot – Choose CDW or Office Max vendor sites.
Kanguru Defender Elite 4GB USB FD	Mfg#: KAR-KDFE-4G Contract: Amerinet Tier 4 VH10213	Deacon Depot – Choose CDW or Office Max vendor sites.
Kanguru Defender Elite 8GB USB FD	Mfg#: KAR-KDFE-8G Contract: Amerinet Tier 4 VH10213	Deacon Depot – Choose CDW or Office Max vendor sites.
Kanguru Defender Elite 16GB USB FD	Mfg#: KAR-KDFE-16G Contract: Amerinet Tier 4 VH10213	Deacon Depot – Choose CDW or Office Max vendor sites.

Recommended Hard Drives	
Brand	**Model**
IBM	Lenovo ThinkPad Secure 160GB

IBM	Lenovo ThinkPad Secure 320GB
IBM	Lenovo ThinkPad Secure 500GB
IBM	Any Lenovo ThinkPad Secure device