Wake Forest University

Standard

When to Engage Information Security

Legal Department / Director of Information Security

Revision History

Revision	Date	Summary	Author
1.0	November 19, 2012	Original Release	Jeff Teague

Wake Forest University
Standard on When to Engage Information Security

Introduction and Purpose

All WFU departments are responsible for understanding when Information Security is engaged for project, work unit, new service related tasks, or investigations. Departments are also responsible for ensuring that individuals are aware of their responsibility to engage Information Security in accordance with this standard.

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

Scope

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

Standard

Information Security can assist with security related issues such as requirements, refining scope, defining security design requirements, defining service level agreements (SLAs), designing controls (detective, preventative, and corrective), evaluating third party vendor control documentation, performing research on legal and industry regulation compliance, and assisting in risk management.

In addition, Information Security must be engaged during the planning of a project, work unit or service creation for the following types of work:

- Access to Electronic Non-Public Information (e-NPI), Critical Financial or Critical Functional Data
  Data associated with e-NPI data or other critical data. This includes data located within WFU, the Internet cloud or at a third party vendor's site. See http://infosec.wfu.edu/standards/ for more information on e-NPI.

- Internet Access
  WFU data, hardware or applications that can be accessed via the Internet. This includes web pages; computers and applications supported by third parties; and any other sites or computers that can be accessed remotely. This does not include WFU faculty, staff, or students with authorized remote access into the WFU network.

- University Safety and Physical Security
  Data associated with technology relating to WFU physical security controls. This includes camera systems, badging, fire systems, and other systems related to the safety and physical security of WFU faculty, staff, students and property.

- Credit Card Payment Processes
  Data associated with any credit card payment processes. Information Security will interface with the Payment Card Industry (PCI) committee and update the committee accordingly on work performed. All requirements will be based upon the PCI standard requirements.

- Legal and Regulatory
  Related to any legal or regulatory action such as Family Educational Rights and Privacy Act (FERPA), North Carolina Identity Theft Act, litigation hold, or other applicable law or regulation

  Information Security may be contacted via a request to infosec@wfu.edu email address.