WAKE FOREST
UNIVERSITY

Cyber Security Incident Response Administrative Policy

Approved By:	Information Systems Leadership Team
Effective Date:	3/3/2016
History:	Approval Date: 3/3/2016
Type:	Administrative Policy
Responsible Official:	Director of Information Security
Review Cycle:	Every Three Years from Effective Date
Last Review Date:	3/3/2016

Policy Statement

This policy provides guidance on responding to potential cyber security events and communicating to appropriate internal and external entities. This standard is applicable to all IT departments or activities, both centralized and decentralized, within the University.

Reason for the Policy

The goal of the Cyber Security Incident Response Administrative Policy is to detect and react to computer security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

Incident Definition

A cyber security incident is an event that, as assessed by IS staff, violates the *Information Security Policy*; *Policy on Responsible and Ethical Use of Computing Resources;* other University policy, standard, or code of conduct; or threatens the confidentiality, integrity, or availability of computing resources and computing systems of Wake Forest University. Incidents may be established by review of a variety of sources including, but not limited to IS monitoring systems, reports from WFU staff or outside organizations and service degradations or outages. Information Systems Security will be the point of contact for all potential incidents and will be responsible for leading the response, declaring the incident and documentation.

Incident Response Reporting

Anyone aware of or suspecting a potential cyber security event can report it by:

- Email infosec.wfu.ed
- Calling the Bridge at 336-758-4357 (HELP) during the hours of M-F, 8am-5pm https://sites.google.com/a/wfu.edu/is-knowledge-base/hours
- Calling University Police at
  - Phone On Campus: 911
  - Cell or Off Campus: 336-758-5911
  - Non Emergency: 336-758-5591

Incident Response Team Composition

In order to investigate, communicate, and mitigate potential incidents, a collaborative team effort is required. While not all team members are involved in all potential incidents, here is the list of potential team members depending on the type and severity of the potential incident:

- Information Security
- Internal Audit
- Privacy Office
- Legal Department
- Campus Life
- Campus Assessment, Response, and Evaluation (CARE)
- Communications & External Relations (CER)
- Information Systems
  - CIO
  - Leadership team
  - Infrastructure
  - Applications Development
  - Client Services
  - Administration
- Executives as necessary such as CFO, Athletics Director, etc.
- Provost, Dean, Chair of Department
- Other impacted schools or departments such as Advancement, School of Business, Law School, Athletics, Finance, HR, Financial Aid, Student Life, etc.

Communication

One key component of any potential cyber security response is insuring that communication is handled in a timely manner and with the appropriate people and organizations. The appropriate members of the Incident response team will be notified and updated on a regular basis. A phone bridge has been established for communication and updates during potential incidents. The phone bridge information is:

1-877-668-4493 Call-in toll-free number (US/Canada)
1-650-479-3208 Call-in toll number (US/Canada)

1-650-479-3208 Call-in toll number (US/Canada)

77575978 Host access code
77037720 Attendee access code

Because of the potential for loss of sensitive information and subsequent reputational loss for the University, information related to potential incidents shall be shared on a need to know basis.

If the potential incident involves sensitive information as defined in the Electronic Non-Public Information Standard or has legal or regulatory reporting requirements, then the Legal Department and Privacy Office must be immediately notified. In these instances, communication to outside entities will be approved by the President, CFO, Provost, General Counsel, or their representative.

This policy is based upon industry best practice, laws, regulations, and contractual requirements including but not limited to the following:

- Gramm-Leach-Bliley Act (GLBA) as it relates to Student Aid
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Social Security Act
- Digital Millennium Copyright Act (DMCA)
- Electronic Communications Privacy Act
- North Carolina Identity Theft Protection Act
- Federal Information Security Management Act (FISMA)
- Law enforcement
- NCREN
- Appropriate contact at attacking location
- Vendors or entities associated with contracts
- Others

Responsibilities

Responsible University Office or Officer

The University Information Technology Partners Council (ITPC) will provide regular advice and guidance to this policy. The Strategic Planning Committee for Information Security provides advice and guidance for policy and general information security.

Under the direction of the CIO, the Director of Information Security is responsible for maintaining and reviewing this policy.

Who Is Governed By This Policy

This policy applies to all IT related activity and departments or individuals that perform IT related functions. This includes both Information Systems and other decentralized IT departments.

Related Policies

N/A

Related Documents

Appendix A - General Process for Cyber Security Incident Response

Highlights of Revisions, by Date

(Revision history by date; i.e., a catalog summarization of key changes to the policy.)

Revision	Date	Summary	Author
1.0	January 2016	Original Release	Joel Garmon

Appendix A

General Process for Cyber Security Incident Response

Information Systems Security is responsible for either performing or delegating all steps below and insuring the tasks are completed and documented.

STEP 1: Identification

Verify that an incident has actually occurred. This activity typically involves the systems administrator and end user, but may also result from proactive incident detection work. If it is determined that an incident has occurred, inform appropriate authorities or regulatory agencies.

STEP 2: Damage Containment and Data Exposure Assessment

Identify an incident response lead and assemble an incident response team charged with limiting further damage from the incident. Conduct a thorough assessment of the type and scope of data exposed following applicable laws, regulation and policy.

STEP 3: Eradication and Recovery

Take steps to remove the cause of the exposure, reduce the impact of the exposure of the sensitive data, and restore operations if the incident compromised or otherwise put out of service a system or network, and ensure that future risk of exposure is mitigated.

STEP 4: Notification

Determine the need to give notice to individuals whose data may have been exposed by the incident. Also evaluate if outside agencies or organizations must be notified.

STEP 5: Follow-up

Identify lessons learned from the incident, implement any remediation needs, and securely store a complete record of the incident.

Documentation for Incidents

A. Where did the incident occur?
B. Who reported or discovered the incident?
C. How was it discovered?
D. Are there any other areas that have been compromised by the incident? If so what are they and when were they discovered?
E. What is the scope of the impact?
F. What is the business impact?
G. Have the source(s) of the incident been located? If so, where, when, and what are they?