*New Standard*

**This standard sets forth the requirements for reporting and responding to information security incidents.**

# NORTH CAROLINA A&T STATE UNIVERSITY

## CHAPTER 700 – INFORMATION TECHNOLOGY

## UNIVERSITY STANDARD US708,<br>INCIDENT RESPONSE STANDARD

### SECTION 708.1 STANDARD STATEMENT

Information Security Incidents have grown in frequency, severity, and methodology, and can represent a significant risk to the University and its Information Resources. North Carolina A&T State University's (N.C. A&T or University) Policy 701, Information Security (ISP) requires the Information Security Incident Response Team (ISIRT) to manage all Information Security Incidents. The ISP also requires the Executive Security Review Team (ESRT) to review incidents that have special legal, policy, and notification requirements, or that pose elevated risk to the university, and all employees, students, and affiliates to promptly report Incidents to Information Technology Services (ITS).

### SECTION 708.2 PURPOSE

This standard sets forth the requirements for reporting and responding to Information Security Incidents at N.C. A&T. Its purpose is to minimize the risk, scope, severity, and damage of Incidents. It ensures that Incidents are promptly reported, and that Incident Response is properly and consistently managed.

### SECTION 708.3 SCOPE

This standard applies to all Information Resources owned or operated by the University or by another organization that provides services to the University. It applies to all employees, students, and affiliates granted use of Information Resources.

### SECTION 708.4 DEFINITIONS

"Breach" means a confirmed Incident in which Confidential, Sensitive, or Controlled Data or an Information Resource has been accessed in an unauthorized manner. A Breach has not occurred if data has been exposed but not accessed.

"Confidential Data" as defined in the ISP means University Data that are protected by federal, state, or local statutes and regulations, industry regulations, provisions in government research grants, or other contractual arrangements, which impose legal and technical restrictions on the appropriate use of institutional information. Updates to this definition in the ISP shall have precedence over the definition in this standard.

“Controlled Data” as defined in the ISP means University Data that are proprietary or produced only for use by members of the university community who have a legitimate purpose to access such data. Updates and revisions to the ISP definitions shall be considered as adopted in this standard.

“High Impact” describes an incident or event whereby Confidential or Sensitive Data was accessed, stolen, modified, deleted, or otherwise compromised; that the University cannot provide one or more critical services to any users; that Confidential or Sensitive Data recovery is unpredictable or impossible;  or that Controlled Data was accessed, stolen, lost or altered, and the actions pose a risk to the University or its Information Resources e.g., theft of data that violates the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), credit card data, corruption of an enterprise database, the loss of campus telephony services, etc.).

“Incident Response” means the steps necessary to prepare for, detect, and analyze any Incident, contain its spread, eradicate traces of infection, compromise, or Vulnerability, restore service, and assess the steps taken after an Incident.

“Information Resource” as defined in the ISP means information owned or processed by the University, or related to the business of the University, regardless of form or location, and the hardware and software resources used to electronically store, process, or transmit that information. Information resources expressly include data, software, and physical assets. Updates and revisions to the ISP definition shall be considered as adopted in this standard.

“Information Resource Custodian” (Custodian) as defined in the ISP, means any university employee authorized to grant access to university data based on delegation from an Information Resource Trustee or Steward, or who have been assigned operational responsibilities for maintaining applicable controls such as data security, physical security, and backup and recovery. Updates and revisions to the ISP definition shall be considered as adopted in this standard

“Information Resource Steward” (Steward) as defined in the ISP, means unit or department leaders with planning and management responsibility for defined information resource data sets, software, or physical assets. Data stewardship responsibilities include data classification, access control, accuracy, integrity, retention, and disposal. Updates and revisions to the ISP definition shall be considered as adopted in this standard.

“Information Security Incident” (Incident) is any attempt to access, use, disclose, modify or destroy University Data, compromise the security, configuration, or operation of an Information Resource, or degrade or interrupt services without authorization, any attempt to interfere with the configuration or operation of an Information Resource, or any violation of the ISP or the University’s Acceptable Use Policy. An Incident may include, but is not limited to, any of the following:

- a Breach, attempted Breach or other unauthorized access of an Information Resource by an employee, student, affiliate or an external entity

- exposure of Confidential, Sensitive, or Controlled Data
- any disruption or attack impacting Information Resources
- any loss or theft of an Information Resource.

“Low Impact” describes an Incident that has no effect on the University’s ability to provide all services or those services that operate at reduced efficiency. Alternatively, it means that no University Data was accessed, exfiltrated, modified, deleted or otherwise compromised, and that recovery can occur with available resources in a predictable time period e.g., the compromise of a small number of accounts in a phishing attack in which the accounts were not used to access University Data, the infection of a small number of computers with virus software or malware in which the software can be eradicated and no data was accessed, modified, or lost or no services were interrupted, etc.).

“Medium Impact” describes an Incident that prevents the University from providing a critical service to a subset of users or that recovery is predictable but requires resources beyond those available during normal operations e.g., a network outage in one building or a virus infection that does not affect data but compromises a large number of computers).

“Sensitive Data” as defined in the ISP means University Data that may not be protected by law or regulation but are considered private and are subject to restricted treatment; Information Resources that may be protected by contracts, third-party agreements, or university policy. Updates and revisions to the ISP definition shall be considered as adopted in this standard.

“University Data” as defined in the ISP means Information Resources that include information created, acquired, maintained, processed or transmitted by or on behalf of N.C. A&T, regardless of form or location, and utilized in the management and operation of educational, research or business activities. Updates and revisions to the ISP definition shall be considered as adopted in this standard.

“Vulnerability” as defined in University Standard US707, Vulnerability Management Standard (VMS), means a weakness in a system, either by software defect or configuration, which can be exploited to perform unauthorized actions. Vulnerabilities may or may not result from and may or may not be corrected by patches. Updates and revisions to the ISP definition shall be considered as adopted in this standard.

## SECTION 708.5 COMPLIANCE

Standards derived from the ISP are mandatory for all employees, students, and affiliates. Failure to adhere to these standards may result in disciplinary action, up to and including dismissal, suspension or expulsion, or termination of privileges.

## SECTION 708.6 RESPONSIBILITIES

Executive Security Review Team

The ESRT is responsible for reviewing investigative results, determining whether a Breach occurred, and identifying appropriate actions to address a Breach. The ESRT may consult with additional leaders as necessary.

Information Security Incident Response Team

The ISIRT is responsible for providing technical expertise to centrally manage all Incidents and provide specialized Incident Response services.

Information Resource Custodians

Custodians shall work with ITS to monitor resources and support Incident Response activities.

Information Technology Services

ITS is responsible for investigating Incidents and determining scope, impact, and the appropriate response. ITS is also responsible for leading preparation, detection, analysis, containment, eradication, recovery, and post-incident processes, for gathering and preserving evidence, and for internal communications regarding Incidents and Incident Response activities.

Information Resource Stewards

Stewards shall work with ITS to monitor resources and support Incident Response activities.

University Police Department

The University Police Department (UPD) is responsible for leading investigations of criminal activities and coordinating with ITS to secure and defend the University's technology environment when criminal activities involve Incidents.

Users

N.C. A&T employees, students, and affiliates (Users) are responsible for notifying ITS of any potential or suspected Incidents and assisting ITS or the ISIRT during the investigation or response as necessary.

## SECTION 708.7 INCIDENT CLASSIFICATION

An Incident shall be classified as Low, Medium, or High Impact based on its functional, informational, and recoverability impact. The Incident shall be classified according to the highest impact across all three factors.

The functional impact describes the University's ability to provide service during the Incident or Incident Response. The impact shall be measured based on the following table.

| Category | Definition |
|---|---|
| Low | The Incident has no effect on the University's overall ability to provide all services to all users or the University can provide all critical services to all users at reduced efficiency.<br>An Incident whose impact is limited to one organizational unit of the University may be considered low impact. |
| Medium | The University is no longer able to provide a critical service to a subset of users. |
| High | The University is no longer able to provide one or more critical services to all, or a significantly large population, of users. |

The informational impact describes theft, loss, or alteration of University Data. The impact shall be measured based on the following table.

| Category | Definition |
|---|---|
| Low | The Incident did not result in the access, exfiltration, modification, deletion or other compromise of any University Data. |
| Medium | The Incident resulted in the modification or deletion of University Data classified as Public. |
| High | The Incident resulted in the access, exfiltration, modification, deletion, or compromise of University Data classified as Confidential, Sensitive, or Controlled.<br>Controlled Data whose access, theft, loss, or alteration poses a risk to the University or its Information Resources, such as infrastructure configuration information, was accessed, modified, deleted, or exfiltrated. |

The recoverability impact describes the ability to recover from the Incident and restore normal operations. The impact shall be measured based on the following table.

| Category | Definition |
|---|---|
| Low | Recovery time is predictable with existing resources. |
| Medium | Recovery time is predictable with resources beyond those available during normal operations. |
| High | Recovery time is unpredictable and additional resources and external assistance are needed.<br>Recovery from the Incident is not possible. |

## SECTION 708.8 REQUIREMENTS

Incident Response is a set of coordinated steps to prepare for and address an Incident. This includes restoring services and normal operations, and using lessons learned from one Incident to prepare for future Incidents. It also includes complying with various laws and regulations in the event of a Breach.

### Section 708.8.1 Preparation

Stewards and Custodians shall maintain accurate inventories of Information Resources. Resources shall be classified according to University Standard US702, Information Resource Risk Classification. Stewards and Custodians shall monitor resources in order to develop baselines of normal activity to be used to detect unusual activity.

Stewards and Custodians shall work with ITS to implement security controls to limit the scope and severity or potential Incidents and address those that occur. These controls shall include contact information for staff and vendor support channels, alternative communication methods, backups of data and system images, antimalware or antivirus software, harden system configuration guidelines, limitations on access and use of privileged accounts, separation of duties, and other measures necessary to secure the resource. ITS shall maintain a secure storage facility to secure evidence and other sensitive material.

Custodians, Stewards, the ESRT, and the ISIRT shall receive annual Incident Response training.

### Section 708.8.2 Detection and Analysis

Stewards and Custodians shall monitor Information Resources for indications or suggestions that an Incident may occur, including following the steps documented in the VMS. Stewards and Custodians shall monitor resources for unusual or unauthorized activity which might indicate that an Incident has occurred or is underway.

Stewards and Custodians shall immediately notify ITS of any potential or suspected Incident. Users shall also notify ITS, the appropriate Steward or Custodian, and their supervisor of any potential or suspected Incident.

If the Incident involves a device under a Steward's, Custodian's or User's control, the device shall be disconnected from the University's network but shall remain powered on for analysis.

When a Steward, Custodian, or User suspect criminal activity in relation to the Incident, the User should notify University Police immediately.

ITS shall investigate the Incident and perform an initial assessment of its scope, severity, and the risk posed to the University and its Information Resources. This shall include collecting relevant data such as the IP addresses of attackers, the identity of threat actors, the mode of operation of the attack, and identifying additional communication channels that might be in use. ITS shall assign an initial classification of Low, Medium, or High Impact. Based on this assessment, ITS shall develop an appropriate initial response plan.

In the event of multiple concurrent Incidents, ITS shall prioritize those that pose the greatest risk to the University.

Incidents with a Low Impact shall be addressed following standard operating procedures as developed by the appropriate Custodian. ITS shall determine if Medium or High Impact Incidents should be addressed following standard operating procedures or if the ISIRT should be convened to respond to the Incident. Senior ITS leadership shall be promptly notified as soon as possible of Medium and High Impact Incidents.

ITS shall work with Stewards and Custodians to monitor environments for a wider scope or severity. ITS shall reassess and reclassify an Incident if additional data indicates a wider scope, greater severity, or a more significant risk to Information Resources. Plans to address the incident shall be updated if the Incident classification changes, or as needed to address additional data.

The ISIRT shall review the initial assessment and classification and revise both as necessary. This may include collection of additional data or the addition of additional staff to complete the response.

During an investigation, ITS staff or the ISIRT shall follow approved procedures to acquire, preserve, secure, and document all evidence to prevent spoliation and support chain of custody requirements. ITS staff or the ISIRT are specifically authorized to take custody of computers, peripherals, data, and other Information Resources in these situations. In any case in which federal, state, local, or campus law enforcement is involved in the investigation or other response processes, the law enforcement agency's need to take custody of Information Resources in order to preserve evidence shall prevail.

### Section 708.8.3 Containment, Eradication and Recovery

In situations where ITS determined that an Incident will be addressed through standard operating procedures, ITS staff shall use these procedures to address the Containment, Eradication, and Recovery steps.

In other situations, the ISIRT shall take steps to stop or contain the Incident before it causes additional damage and prevent data exfiltration. The goal of containment shall be to protect the University and its Information Resources. This may require disconnecting some resources from the network, either physically, virtually, or logically, shutting down services, blocking communications from an attacker, locking accounts, resetting passwords, or other steps. As part of these steps, the ISIRT shall evaluate the need to keep critical services online and the need to provide temporary solutions.

Once the Incident has been contained, the ISIRT shall eradicate all traces of malware or viruses, repair compromised and damaged equipment, change passwords or other access credentials, and take other steps as necessary to secure the environment. This includes following the steps to remediate any Vulnerabilities that contributed to the Incident as documented in the VMS. This may also include modifying standard operating procedures. Stewards and Custodians shall work with the ISIRT to complete these tasks. These changes shall follow the requirements documented in University Standard US703, Information Technology Change Management. The ISIRT shall perform an analysis after eradication to verify its successful completion and shall address any remaining issues.

After completion of the eradication process, the ISIRT shall focus on recovery to restore resources to normal operations. This may include reimaging computers, restoring systems from backup, replacing damaged or compromised files, or other necessary steps.

Detection, analysis, containment, eradication and recovery processes may overlap or may be iterative in actual implementation.

### Section 708.8.4 Post-Incident Activity

As the final step in responding to the Incident, ITS shall convene a meeting to capture knowledge gained during the response. Topics for this meeting shall include a review of the nature of the Incident, steps taken during the response, and may include changes in security controls or additional measures to address similar events, future training opportunities, and changes in policies or standard operating procedures. These outcomes shall be reviewed by ITS to improve preparation for future Incident Response.

### Section 708.8.5 Breach Determination

The ESRT shall examine investigation results if data was exposed to determine if a breach has occurred. If the ESRT determines that a breach occurred, it will coordinate breach management with the affected department or division.

### Section 708.8.6 Incident Response Communications

During an Incident Response, communications may need to occur quickly, utilizing established relationships between University leaders, staff, and departments as well as external groups such as vendors, Incident Response teams of other organizations or law enforcement. All external communications with the media or public related to any Incident shall be coordinated through University Relations and the Vice Chancellor of Information Technology, or their delegates. ITS shall distribute internal communications to warn the University community of imminent threats, solicit information, or provide notice of service interruptions.

### Section 708.8.7 Evidence Retention

Evidence collected from an Incident Response where criminal activity or compromise of an Information Resource is suspected shall be retained in a secure location until law enforcement and/or the Office of Legal Affairs, in consultation with the Vice Chancellor for ITS, determine that it is no longer necessary to pursue legal action or assess the Incident. Evidence collected by ITS is other cases shall be retained in a secure location until assessment of the Incident is completed.

## SECTION 708.9 EXCEPTIONS

This standard does not apply to authorized actions taken in a controlled laboratory environment used for instruction or research which would otherwise qualify as an Incident. These environments shall be segmented or physically separated from the rest of the N.C. A&T network. Segmentation of these environments shall include limitations on access from said environment to other parts of the University network and the Internet. Limitations shall be developed in cooperation with and approved by ITS before the environment is connected to any N.C. A&T network. Physically separated equipment shall remain physically separate and shall not be connected to any N.C. A&T network without ITS approval.

## STANDARD HISTORY:

Eff. [initial effective date of policy; this is when it has received final approval for implementation]

**AUTHORITY:** Chancellor

**STANDARD OWNER:** Vice Chancellor for Information Technology

**RESPONSIBLE OFFICE:** Information Technology Services

## RESOURCES:

UNC Policy 1400.1 Information Technology Governance
ISO 27002:2013 Code of Practice for Information Security Controls
N.C. A&T Policy 701, Information Security

N.C. A&T Policy 702, Acceptable Use
N.C. A&T Standard US702, Information Resource Risk Classification
N.C. A&T Standard US703, Information Technology Change Management
N.C. A&T Standard US707, Vulnerability Management
NIST Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide