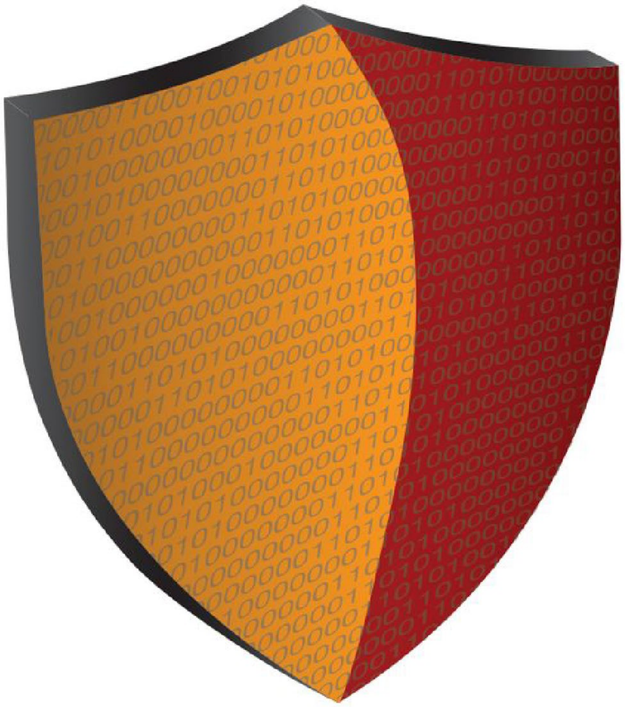


Virginia Tech Guide for Cyber Security Incident Response v5.4

3/20/2023

IMPORTANT NOTE: If an incident is deemed to be illegal or life threatening, contact the VA Tech Police: 540-231-6411, or Emergency: 911.

ABSTRACT

This document assists university personnel in establishing cyber incident response capabilities and handling incidents efficiently and effectively. It provides a guide for cyber incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.

The IT Security Office can be reached by emailing itso-g@vt.edu or calling 540-231-6020

Table of Contents

Section 1: Introduction

Authority

Oversight of the security of university information technology resources and information is entrusted to the Vice President for Information Technology by the Virginia Tech Board of Visitors.

In 2007, the Board of Visitors passed a resolution (https://bov.vt.edu/assets/june_4-2007.pdf , Attachment V) requiring the Vice President for Information Technology to ensure compliance with established security standards throughout the University. The Vice President for Information Technology and CIO has given the IT Security Office (ITSO) full authority to act in a manner to protect the integrity, confidentiality, and availability of Virginia Tech's information technology infrastructure.

Virginia Tech Policy 7010 - "Policy for Securing Technology Resources and Services," gives the ITSO the authority to respond to threats to University networks, systems, and services.

The University Information Technology Security Program Standard of 2012 states that evaluating and reporting cyber security incidents is important to ensure information security events and weaknesses associated with information systems are communicated in a manner that will allow timely corrective action to be taken. Information Technology is responsible for:

- Maintaining an incident response procedure document
- Maintaining the Computer Incident Response Team (CIRT) to carry out these procedures
- Arranging for intake of reports of suspected IT security exposures of university data and other suspected cyber incidents.

The ITSO manages and coordinates detection, identification, containment, eradication, and recovery efforts of reported cyber security incidents with Virginia Tech departments' IT personnel. The IT Security Officer also has the authority to classify threats as a risk to the enterprise and can activate the VT-CIRT team at his discretion. **The CIRT Team will only be activated if a cyber security incident has been identified as affecting University IT systems/services at an enterprise or a multi-departmental level.**

Purpose and Scope

This publication seeks to assist university personnel in mitigating the risks from cyber security incidents by providing a practical guide for responding to incidents effectively and efficiently. This document includes guidelines on establishing an effective cyber security incident response program, but the primary focus of the document is to provide assistance with detecting, analyzing, prioritizing, and handling incidents.

This document is not intended to replace Continuity or Disaster Recovery Planning. ***It is not intended to be used as a detailed list to accomplish every task associated with cyber security incident handling and response.*** Rather, the document is intended to provide a framework and processes by which consistent approaches can be developed and resource allocations can be made for incident response incidents.

This document addresses only incidents that are computer security-related, not those caused by natural disasters, power failures, etc.

This document applies to university-owned computers and technology devices connected to the Virginia Tech network. All University locations are covered by this document.

This document is intended to provide guidance to address cyber security incidents that have impacts that affect the University's operational, financial, or reputational standing and/or the ability to comply with regulatory or legal requirements.

Audience

This document has been created for the VT cyber incident response team (CIRT), system and network administrators, security staff, technical support staff, chief information security officer (CISO), chief information officer (CIO), computer security program managers, and others responsible for preparing for or responding to cyber security incidents at Virginia Tech.

Document Structure

The rest of this document is arranged as follows:

Section 2 discusses the need for cyber incident response capabilities, and outlines possible cyber incident response team structures as well as other groups within the organization that may participate in cyber incident response handling.

Section 3 provides guidelines for effective, efficient, and consistent incident response capabilities and reviews the cyber security incident response elements.

- Appendix A – VT Cyber Incident Response Teams Organizational Chart
- Appendix B – Communication Workflow for Sensitive Data Exposure
- Appendix C – CIRT Team, IT Council, Compliance Officers Directories
- Appendix D – Incident Handling Checklist - Unix, Linux and Windows Forensics checklists
- Appendix E – Detection and Analysis Information Gathering Outline
- Appendix F – Communication Plan Worksheet
- Appendix G – Internal Audit Guidelines for unacceptable computer use
Appendix H – University Policies and Standards
- Appendix I – Workflow Diagram for Incident Escalation Appendix
- J – Contact information for local police and FBI
- Appendix K – Generalized Cyber Incident Escalation and Workflow Diagram
- Appendix L – Acronyms
- Appendix M – Step by Step Cyber Incident Response

Section 2: Cyber Incident Response Capabilities

A cyber security incident is defined by the Department of Homeland Security as an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.[1] An incident could be either intentional or accidental in nature.

Examples of cyber security incidents (hereafter may be referred to as "cyber incident" or "incident") may include, but are not limited to:

- An incident in which an attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- An incident in which users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An incident where an attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- An incident where a user provides or exposes sensitive information to others through peer-to- peer file sharing services.

Successful incidents similar to those noted above have occurred at Virginia Tech. These incidents have caused financial and reputational harm, disrupted daily operations, and created compliance issues with state and federal laws. Establishing cyber incident response capabilities at Virginia Tech ensures systematic (i.e., following a consistent cyber incident handling methodology[1]) and coordinated actions are taken. Incident response helps personnel to minimize loss or theft of information and disruption of services caused by cyber incidents.

Incident response capabilities also build institutional resilience. Information gained and lessons learned during incident handling can help better prepare for dealing with future incidents.

Mission

One of the elements of Virginia Tech's Information Technology mission is to provide, secure, and maintain information systems, allowing the University to accomplish its mission.

To support the University's mission, Information Technology has developed a guide for implementing cyber security incident response plans. To aid in the coordination of response activities, Information Technology has formed a Cyber Incident Response Team (CIRT). The CIRT mission is to:

1. Limit the impact of cyber incidents in a way that safeguards the well-being of the University community.

[1] From https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/coordination-of-federal- information-security-policy.pdf - 44 U. . Code § 3552S

2. Protect the information technology infrastructure of the University.

3. Protect sensitive University data from disclosure, modification, and exfiltration.

4. Collect the information necessary to pursue investigation(s) at the request of the proper University authority.

Strategy and Goals for Cyber Incident Response

Timely and thorough action to manage the impact of cyber incidents is a critical component of the response process. The response should limit the potential for damage by ensuring that actions are well known and coordinated. Cyber incident response goals are:

- To protect the well-being of the University community.
- To protect the confidentiality, integrity, and availability of University systems, networks and data.
- To help University personnel recover their business processes after computer or network security incidents.
- To provide a consistent response strategy to system and network threats that put Virginia Tech data and systems at risk.
- To develop and activate a communications plan including initial reporting of the incident as well as ongoing communications as necessary.
- To address cyber related legal issues.
- To coordinate efforts with external Computer Incident Response Teams.
- To minimize the University's reputational risk by notifying appropriate University officials of cyber incidents that may become high profile events and implementing timely and appropriate corrective actions.

To achieve these goals, Information Technology has adopted security best practices derived from standardized incident response processes such as those published by the National Institute of Standards and Technology (NIST) Special Publication 800-61 and other authorities.

The specific incident response process elements that comprise the VT Cyber Incident Response Plan include:

- Preparation: Maintaining and improving incident response capabilities and preventing incidents by ensuring that systems, networks, and applications are sufficiently secure.

- Identification: Confirming, characterizing, classifying, categorizing, scoping, and prioritizing suspected incidents;

- Containment: Minimizing loss, theft of information, or service disruption;

- Eradication: Eliminating the threat;

- Recovery: Restoring computing services quickly and securely;Post-incident activities: Assessing response to better handle future incidents through utilization of reports, “Lessons Learned,” and after-action activities, or mitigation of exploited weaknesses to prevent similar incidents from occurring in the future.

These six elements of Cyber Incident Response will be defined in detail in section 3.

Cross-cutting elements present throughout incident response handling include:

- Communication: Notifying appropriate internal and external parties and maintaining situational awareness;
- Analysis: Examining available data to support decision-making throughout the incident management lifecycle; and
- Documentation: Recording and time-stamping all evidence discovered, information collected, and actions taken from Identification through Post-incident activities.

University Authority for Cyber Incident Response

The following University organizations act as University Authorities; those who are authorized to make requests and decisions regarding cyber security incident response at Virginia Tech.

- Vice President for Information Technology and Chief Information Officer (CIO) – empowered to respond to IT security incidents by BOV Resolution "Information Technology Security and Authority". https://bov.vt.edu/assets/june_4-2007.pdf

- Information Technology Security Officer (ITSO) – delegated authority by CIO to decide whether to activate CIRT, notifies Incident Governance Team of decision

- VT CIRT Governance Team – a broad range of University stakeholders (see Appendix A).

- University Legal Counsel – any law enforcement/legal actions, questions about information disclosure, legal aspects of the investigation

- University President – personnel actions for staff

- Executive Vice President and Provost – personnel actions for faculty

- University Internal Audit – data integrity of critical University data, compliance with University procedures and fraud investigations

- Division of Student Affairs/Student Conduct – offenses by Virginia Tech students

- Virginia Tech Police Department – criminal matters
- Data Trustees/Stewards – sensitive or non-public data access and governance. Data trustees and stewards are listed at https://it.vt.edu/resources/policies/adms.html .

NOTE: Requests from local, state, or federal law enforcement officials do not necessarily constitute proper authority. All requests from these agencies must first be made to University Counsel before contacting any university departmental personnel.

Any of the following requests from local, state or federal law enforcement agencies ***must be authorized by University Legal Counsel prior to issuance:***

- ***Warrant - If you are presented with a warrant that has been authorized by University Legal Counsel, you should comply immediately with the request. Notify your supervisor and the Campus Police unless advised otherwise by law enforcement or University Legal Counsel.***

- ***Subpoena - If you are presented with a subpoena that has been authorized by University Legal Counsel, comply with the request. Notify your supervisor unless you are advised otherwise by Legal Counsel.***

- ***Freedom of Information Act – University Legal Counsel will advise how requests should be honored.***

Cyber Incident Response Teams

The VT Cyber Incident Response Team (VT-CIRT) is composed of current members of the IT Security Office staff and Division of Information Technology contacts from Secure Identity Services (SIS), Network Infrastructure & Services (NI&S), IT Experience & Engagement aka 4HELP, Enterprise Systems, Advanced Research Computing (ARC) and Collaborative Computing Solutions (CCS); as well as University college and departmental representatives that make up the IT Council, and University Compliance Officers. See Appendix C for contact information for VT-CIRT members.

Cyber Incident Response Governance Team Composition

The cyber incident response governance team is a new group that has been formed to provide oversight for cyber incident response. The Cyber Incident Response Governance Team is composed of the following University stakeholders:

- Vice President for Information Technology and CIO
- Information Technology Security Officer
- University Legal Counsel
- University Internal Audit
- VT Police Department
- Data Trustees/Stewards
- University Relations

VT's Approach to Cyber Incident Response:

This section provides guidelines for establishing incident response capabilities, and advice on maintaining and enhancing existing capabilities in the event of a cyber incident.

Reporting a Cyber Incident

A cyber incident is an event that poses a threat to the integrity, availability, or confidentiality of an IT system. Cyber incidents should be reported immediately to the IT Security Office or as soon as possible after discovery. The ITSO or designee will act as the Incident Response Manager (IRM) for all reported cyber incidents. The ITSO, with the assistance of the reporting entity will work together to coordinate all aspects of the incident response process. The reporting entities must coordinate with the ITSO (or designee) prior to initiating any actions during the investigation or in response to information security incidents. **All communications regarding cyber incidents must be conducted through channels that are known to be unaffected by the cyber incident under investigation.**

Cyber incidents can be reported in several ways including by email, phone, in-person, or by initiating a Service Now (SN) trouble ticket.

IT Security Office Contact information: itso-g@vt.edu or 540-231-6020 - for a list of IT Security Office staff contact information, see Appendix C.

Examples of incidents that should be reported immediately include, but are not limited to:

- A virus/worm affecting multiple systems;
- Intrusion or damage to;
    - Web site or page,
    - Computer system or network,
    - Wireless access,
    - Cell phones, smartphones
    - Laptops, tablet computers
    - Fax machines,
    - Voice mail, and
    - Voice over IP (VOIP) systems.

See Appendix J for further guidance on reporting cyber incidents.

Early notification allows the ITSO and affected departments time to gather as much information as possible when evaluating potential cyber incidents. **Also, certain data types (student, financial data) have strict notification timeline requirements. See Appendix C.** Information that should be gathered and shared when reporting cyber incidents includes:

- Contact information of affected individuals
- IP address, hostname, or location of system(s)
- In the case of a website intrusion, the specific URL(s)
- Disclosure of data that may be included on the system. This is particularly important if this data may include social security numbers, credit card numbers, bank account numbers, debit card numbers, driver's license numbers, passport numbers, medical information, or FERPA data.
- Disclosure of the system's criticality, as noted on its most recent IT risk assessment.
- A description of the incident that includes a timeline and identification/detection details.

Prompt reporting may also help reduce common risks associated with cyber incidents, including:

- Physical safety risk: As the "Internet of Things" becomes more prevalent in monitoring physical facilities, a cyber attack against networked devices could cause physical harm to individuals.
- Regulatory risk: Compliance with federal and state legislation regarding the protection of information. This includes data and systems that fall under but not limited to GLB (Gramm-Leach-

Bliley Act), HIPAA (Health Insurance Portability and Accountability Act), FERPA (Family Educational Rights and Privacy Act, ITAR (International Traffic in Arms Regulations), PCI-DSS (Payment Card Industry Data Security Standard), federal/state data breach notification laws, and the Patriot Act.

- Operational risk: Failure to protect systems and data can cause disruptions to critical daily operations.
- Financial risk: There may be costs associated with lost data, restoring systems, and data breach notifications.
- Reputational risk: There may be a negative impact on confidence in a system or a negative impact on the university's reputation.

Cyber Incident Response Procedures

Once an incident report has been received, the ITSO will confirm details surrounding the incident through the identification, detection, and analysis phases of incident handling. Different types of incidents merit different types of response strategies, but generally:

- If an incident is confirmed, the ITSO will coordinate actions through the CIRT Governance Team and the CIRT Team.
- If an incident cannot be confirmed, the ITSO will make mitigation recommendations to the reporting entity.

The ITSO, CIRT teams, and/or the IRM (**I**ncident **R**esponse **M**anager) shall categorize the incident according to type and potential impact(s). The incident shall then be classified and responded to in order of priority.

- If immediate action is required, the ITSO will begin coordinated incident response activities. **NOTE:** The CIRT will only be activated if a cyber incident is affecting University IT systems/services at an enterprise or a multi-departmental level.
- If immediate action is not required, the ITSO will work with the reporting entity to determine appropriate response actions.

In the case of multiple cyber incidents occurring simultaneously, the ITSO, CIRT Teams, and/or the IRM will classify the incidents according to their immediate and potential adverse effects and prioritize recovery and investigation activities according to the severity of these effects.

Communications and Information Sharing about a Cyber Incident

Communication is an essential part of cyber incident response. Because communications regarding a cyber incident often need to occur quickly, it is vital to build relationships and establish suitable means of communication between the ITSO and other groups, both internal (e.g., human resources, legal) and external (e.g., other incident response teams, law enforcement). University departments should proactively develop internal cyber security incident communication guidelines.

Once an incident is confirmed, the ITSO and the CIRT Governance Team will work with University Relations to coordinate information sharing so that only the appropriate information is shared with the appropriate parties.

A communication plan is mandatory whenever a breach of Personally Identifiable Information (PII) has been confirmed. Appendix B provides a workflow diagram for communications required when there is an exposure of sensitive data.

A communication plan should identify internal and external communication needs, and how these needs will be addressed. Smaller events may only require internal communications, while larger events may require interaction with external stakeholders. The approach to communications should be tailored depending on the stakeholders.

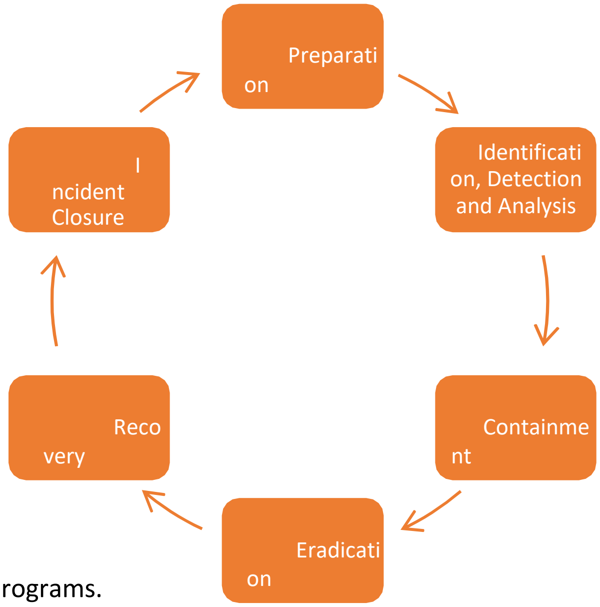
The communication plan should be activated as soon as possible after a cyber incident has been confirmed. Appendix F provides a worksheet to assist in formulating a communication strategy for sharing information in the event of a cyber security incident.

Section 3 provides more detail about developing a cyber incident communications plan.

Section 3: The Incident Response Processes

This section describes the major phases of the incident response process—preparation, detection and analysis, containment, eradication and recovery, and post- incident activity.

Appendix D provides a checklist of major steps to be performed during response and handling of an incident. The checklist does not dictate the exact sequence of steps that should always be followed. Appendix D also provides Unix/Linux and Windows Operating Systems Checklists for responding to system compromises.



Preparation

Preparation is fundamental to the success of incident response programs.

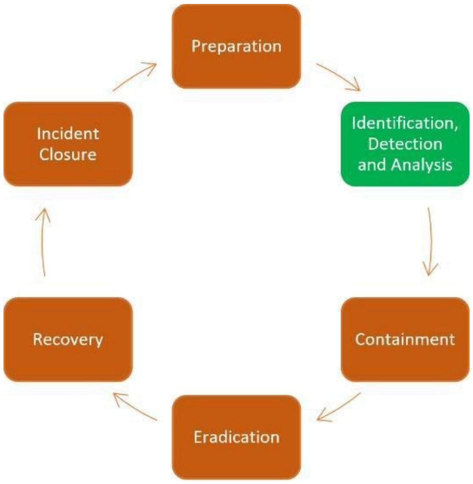
Incident response methodologies typically emphasize the proactive and ongoing use of tools, training, and processes necessary for preventing incidents by ensuring that systems, networks, and applications are sufficiently secure.

Many of the necessary tools and training are available on the IT Security Office website http://security.vt.edu.

University colleges and departments will conduct an annual IT Risk assessment and participate in an annual tabletop exercise using this guide as a reference. Exercise results will be used to determine the effectiveness of this guide. The benefits of conducting an IT Risk Assessment include identifying applicable threats, including organization-specific threats. Each risk is categorized and prioritized to determine if risk can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasize monitoring and response activities for those resources. Templates and training are at the IT Security Office   website: https://security.vt.edu/policies/itra.html

Conducting an IT Risk Assessment enables departments to correlate IT resources with mission critical business processes and services. Using that information, it then becomes possible to characterize interdependencies and the consequences of potential disruptions, as well as to generate plans to eliminate or ameliorate risks. See https://security.vt.edu/policies/itra.html .

Identification, Detection, and Analysis



Early steps taken to detect, verify, investigate, and analyze an incident are important to developing an effective containment and eradication strategy. Once an incident has been confirmed, resources can be assigned to investigate the scope, impact, and response needed. The detection and analysis phases determine the source of the incident and preserve evidence.

The general steps required for incident identification, detection, and analysis are to:

1. Review Internal Audit guidelines for department personnel actions with regard to unacceptable computer use and other cyber security incidents - See Appendix H.
2. Determine whether an incident has occurred.

Coordination between the IT Security Office and the affected department is important to make sure that steps taken to verify the incident do not alter data that will be needed for further investigation.

Detection and Analysis

The IT Security Office will work with the affected department to quickly analyze and validate each incident, and perform an initial assessment to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited). The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.

A coordinated investigation may be required once an incident has been confirmed. The IT Security Office will identify and assign an individual to be the Incident Response Manager (IRM). The IRM will lead the incident response, is the point of contact for all matters relating to the incident, and is responsible for coordinating the data required for documenting the investigation and gathering evidence. In some cases, Federal, State, or local law enforcement may be involved in an incident investigation. See Appendix J for contact information for the Federal Bureau of Investigations (FBI), Department of Homeland Security (DHS), state, campus, and local police.

Inter-departmental Cooperation Guidelines

University personnel may be alerted to a threat from an internal or external source. It is important to notify the IT Security Office once a threat has been detected.

- **The local systems administrator is responsible for fixing the problem on the machine(s)** The IT Security Office may also detect a threat and alert the system custodian of record for the hardware or Ethernet port connection.

- **All incidents should be handled by departmental IT staff with the support of the IT Security Office and, if necessary, the CIRT.**

See Appendix E: Compromise Questionnaire and Information Gathering - Information Needed from the User, and Appendix J: Guidelines for Reporting a Cyber Incident.

Incident Categorization, Classification, and CIRT Activation

The incident type and impact will determine the level of response needed by the University. The IT Security Office will work with departments to determine the appropriate response for each confirmed incident. The general steps required for incident categorization and classification are:

1. Categorize the incident based on type of incident, security objective, and impact.
2. Classify the incident as a local or enterprise incident.
3. Prioritize handling of the incident based on the VT CIRT Incident Response Classification Matrix
4. Activate CIRT if necessary
5. Report the incident to the appropriate internal personnel and external organizations.

Common Categories of Cyber Incidents

Incident Type	Description
Unauthorized Access	When an individual or entity gains logical or physical access without permission to a university network, system, application, data, or other resource.
Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Malicious Code	Successful installation of malicious software (e.g., a virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software.
Improper or Inappropriate Usage	When a person violates acceptable computing policies.
Suspected PII Breach	If an incident involves personally identifiable information (PII) a breach is reportable by being merely **Suspected**. (Suspected PII incidents can be resolved by confirmation of a non-PII determination.)
Suspected loss of Sensitive Information	An incident that involves a suspected loss of sensitive information (not PII) that occurred as a result of Unauthorized Access, Malicious Code, or Improper (or Inappropriate) Use, where the cause or extent is not known.

Source: Incident Response and Management: NASA Information Security Incident Management

Impact Definitions

	Potential Impact		
Security Objective	**Low**	**Medium**	**High**
Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability: Ensuring timely and reliable access to and use of information	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Source: FIPS Publication 199

Once an incident is classified, it is important to categorize the incident as a local or enterprise event.

Local events represent a risk to Virginia Tech systems, networks, and data but are confined to a single or small number of departmental systems. An example of a local issue would be malware discovered on a departmental desktop or server. Local issues may lead to data breaches if unencrypted sensitive data is stored on the compromised systems. Most cyber threats are identified, contained, and eradicated through coordinated efforts between the ITSO and affected departments. Local events are the most common type of attack observed at Virginia Tech.

Enterprise events are wider in scope and affect multiple university departments, colleges or divisions. These attacks disrupt University wide operations or endangers high risk data. Enterprise issues may require the activation of the Cyber Incident Response Team (CIRT). CIRT team members may be drawn from many departments across the university and have knowledge of critical systems that can be leveraged to protect Virginia Tech IT assets during an enterprise incident.

When multiple incidents occur simultaneously, the most serious or highest potential impact incidents should be handled first.

The incident classification is performed by the Incident Response Manager (IRM) using the VT CIRT Incident Response Classification Matrix.

VT CIRT Incident Response Classification Matrix

Classification Level (3=Most Severe)	Typical Characteristics	Impact	Response	Activate CIRT?
3	DDoS attack against University Servers. Attacks against network infrastructure. Network disruption for a large segment of the VT population	An enterprise-wide attack involving multiple departments requiring local and enterprise administrator support from the affected departments.	CIRT directs, response coordinated by ITSO. VT senior management, local sysadmin involved. Possible Legal Counsel, Law Enforcement involvement	Yes
2	Affects data or services for a group of individuals and threatens sensitive data, or involves accounts with elevated privileges with potential threat to sensitive data	Compromised Banner, Exchange, Active Directory, domain controller system administrator account, or Learning Management System (LMS) administrator account compromise	Response coordinated by ITSO. Local Sysadmin. CIRT advised, Legal Counsel notified if PII breach.	Advised
	Affects data or services of a single individual, but involves significant amounts of sensitive data	Faculty desktop with University defined sensitive data compromised, physical theft of computer/computer equipment		No
1	Affects data or services of a group of individuals with no sensitive data involved	Compromise of an account with shared folder access	Local sysadmin, ITSO notified, event logged, progress monitoring, Standard forensics performed if local admin is unable.	No
	Affects data or services of a single individual with no sensitive data beyond their own involved; focus is on correction and/or recovery and education/future prevention	Compromised faculty machine w/no University defined sensitive data etc.		No
0	Occurrences of very minor or undetermined focus, origin and/or effect for which there is no practical follow-up	Network scans, personal firewall log reports, Snort reports, Tripwire, IDS/IPS reports	ITSO monitors periodically, periodic summaries, vulnerability database maintenance, sends reports to central logging facility for trending weekly/monthly reports.	**No**

CIRT Activation

The CIRT will only be activated if a cyber incident has been confirmed to be affecting University IT systems/services at an enterprise or a multi-departmental level. Attacks against departmental servers do not necessarily require CIRT activation. Local events may be escalated to enterprise events if evidence warrants. The ITSO has the authority to classify incidents as an enterprise threat. The ITSO and the CIRT Governance Team have authority to activate the CIRT.

Communications Plan

A communications plan is essential when dealing with a confirmed cyber incident. A good communication plan can help limit confusion and increase responsiveness by sharing action plans, updating University stakeholders, and providing transparency throughout the process. The plan should identify the stakeholders, those authorized to speak about the incident, the communication channels, a schedule of communication as well as procedures for notifying external organizations that are directly involved in the incident. A communications plan can reduce conflicting messages and focus efforts.

University Relations, Information Technology, and the appropriate stakeholders must develop a communications plan whenever a breach of Personally Identifiable Information (PII) has been confirmed. A communication workflow diagram for PII exposure is available in Appendix B.

Potential Stakeholders

- VP for Information Technology and CIO
- IT Security Office Staff
- Data Trustees/Stewards
- CIRT Members
- Departmental Management
- Departmental IT Staff
- University Legal Counsel
- University Relations
- Vendors
- Office of Emergency Management
- Faculty and Staff
- Students
- Law Enforcement Agencies
- Members of Virginia Tech's technical support community
- Outside agencies' Internal Audit
- Internal Audit
- Media

Plans should include the following elements:

- List of those authorized to speak about the incident to university stakeholders and the media
- Clear protocols for message approval, to ensure accuracy
- communication channels for internal and external stakeholders (Email, Listservs, Google groups, phone conferences, Learning Management System, Blogs, Wikis, social media)
- Planned frequency of communications between internal stakeholders
- Planned frequency of communications with external stakeholders
- Notification procedures for external organizations directly involved in incident

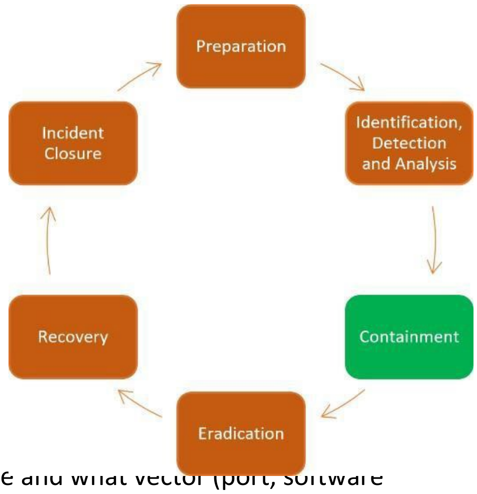
Containment, Eradication and Recovery

Containment

Containment procedures attempt to actively limit the scope and magnitude of the attack. A vulnerability in a particular computer architecture can be exploited quickly. Containment involves acquiring, preserving, securing, and documenting all evidence.

Containment has two goals:

- Prevent data from leaving the network via the affected machines.
- Prevent attackers from causing further damage to Virginia Tech information technology assets.



The ITSO assigns a high priority to determining who the attackers are and what vector (port, software vulnerability, etc.) they are using to attack Virginia Tech hosts. Once this information is obtained, the ITSO will request a router block or physical disconnection to temporarily prevent an IP address, port or both from connecting to the VT network. This may disrupt other normal traffic, but this disruption will be kept to a minimum. Containing a cyber incident has a higher priority than maintaining normal business traffic.

The following actions are taken during the containment phase:

Coordinate all activities with the local system administrator.
Possible actions include:

- Upon direction by the IRM, the local system administrator can proceed to repair the system as needed to return to normal business operations.
- Consulting provided by the ITSO to the local system administrator. The ITSO will remain available to provide consulting support during the repair process.
- The deployment of a small team from the ITSO with the appropriate expertise to the site.
- Securing the physical area on site if necessary.
- Using Appendix E: *Compromise Questionnaire and Information Gathering* to guide documentation.
- A review of the information provided by the system administrators.
- Not allowing the system to be altered in any way. Maintaining a low profile in order to avoid tipping off the attacker.
- Using a trusted system binary kit (Unix/Linux, Windows) to verify the system binaries have not been compromised.

- Making a forensic copy of the system for further analysis. Ensuring that any backup tapes are in a secure location.

Determine risk of continued operation. Possible actions include:

- Disabling network access but leaving the system up. Disabling the port if the attack is ongoing or if the compromised system is attacking another site. The Network Team should utilize available tools to identify and disable the port.
- Making a recommendation to the local management (faculty member, department head, dean, supervisor, etc.) regarding whether the affected system(s) should remain online. Attempting to restore operations as quickly as possible. However, if the compromised system threatens the integrity of the network or systems connected to the network, it should be disconnected from the net as soon as possible.
- Changing all user and system credentials on the affected machine(s).

Backup the system.

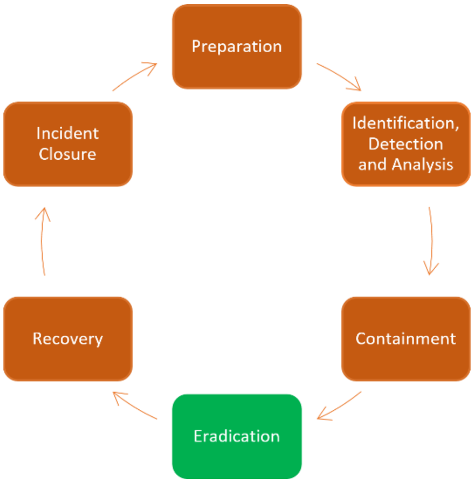
- In some cases, a forensic image disk will be requested by law enforcement or by the office of Legal Counsel. Contact the ITSO to initiate the forensics process.
- Use network backup systems to determine what files were changed during the event

Eradication

Eradication is the removal of malicious code, accounts, or inappropriate access. Eradication also includes repairing vulnerabilities that may have been the root cause of the compromise. We strongly recommend a complete re-installation of the OS and applications.

The general steps involved in the eradication phase of incident response are to:

- Define eradication benchmarks
- Consult various checklists for compromises. See Appendices D, E for general information
- Identify and mitigate all vulnerabilities that were exploited
- Remove malware, inappropriate materials, and other components
- If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps to identify all other affected hosts, then contain and eradicate the incident for them
- Reinstall OS, apply patches, reinstall applications, and apply known patches

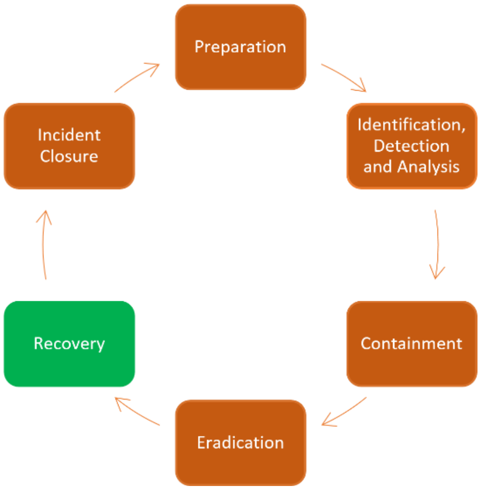


Recovery

Once the incident has been contained and eradicated, recovery can start. This phase allows business processes affected by the incident to recover and resume operations.

The general recovery steps are:

1. If there was sensitive data on the affected machine, go to step 2. If there was not, go to step 4.
2. Follow the flow chart steps in Appendix B.
3. Reinstall and patch the OS and applications. Change all user and system credentials.
4. Restore data to the system.
5. Return affected systems to an operationally ready state.
6. Confirm that the affected systems are functioning normally.
7. If necessary, implement additional monitoring to look for future related Post-Incident Activity.

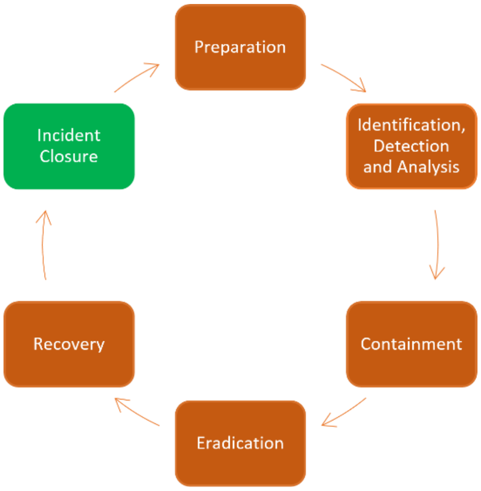


Incident Closure

Documentation of a cyber incident and the steps taken to mitigate issues encountered are important. The documentation offers an opportunity to improve Incident Response processes and identify recurring issues. Most local issues can be properly documented using the University's 4Help trouble ticket system.

Certain cyber incidents should be documented more thoroughly when their impact warrants. The ITSO will identify those local incidents that should be more thoroughly documented. A follow up report and documentation is required for all enterprise level incidents.

Follow-up reports document the incident and include the lessons learned in order to preserve and expand knowledge. Reports are produced by the IT Security Office and/or the CIRT teams depending on the incident. The report should include:

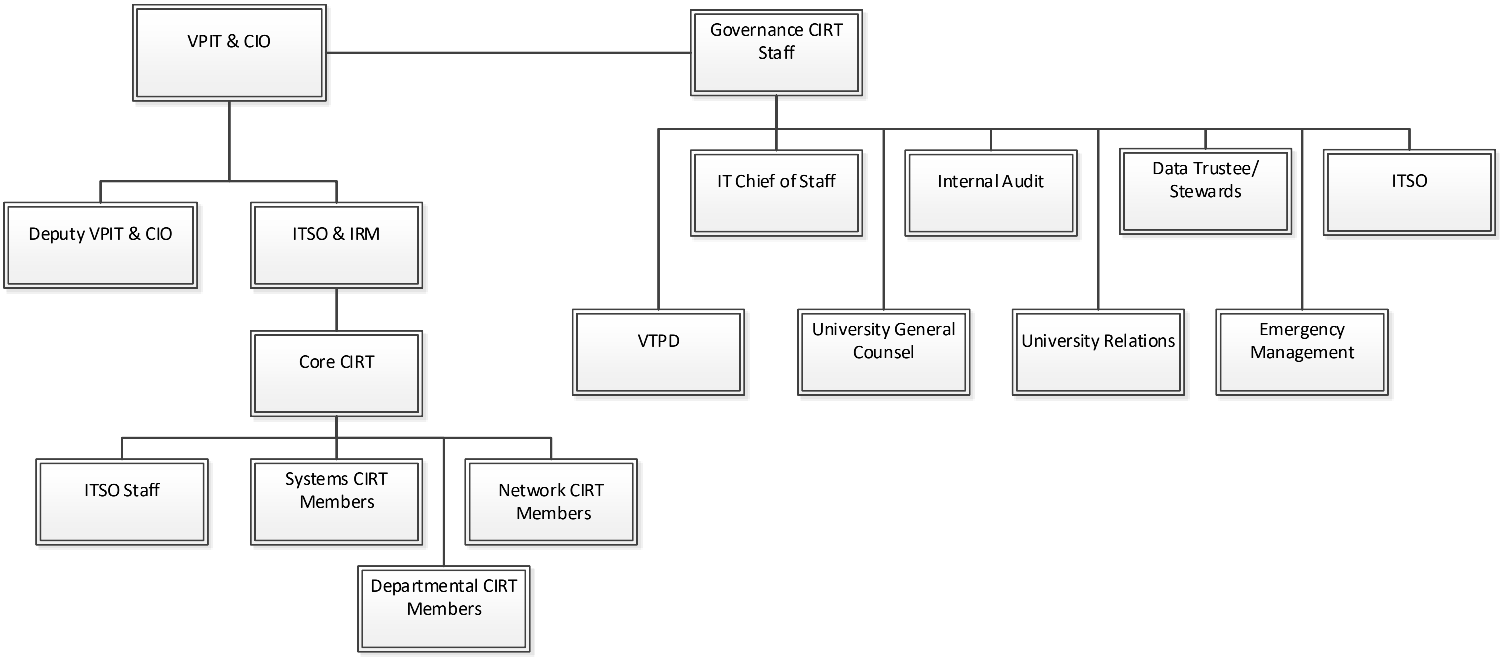


- Information about the incident type
- A description of how the incident was discovered
- Information about the systems that were affected
- Information about who was responsible for the system and its data
- A description of what caused the incident
- A description of the response to the incident and whether it was effective
- Recommendations to prevent future incidents
- A discussion of lessons learned that will improve future responses
- A timeline of events, from detection to incident closure

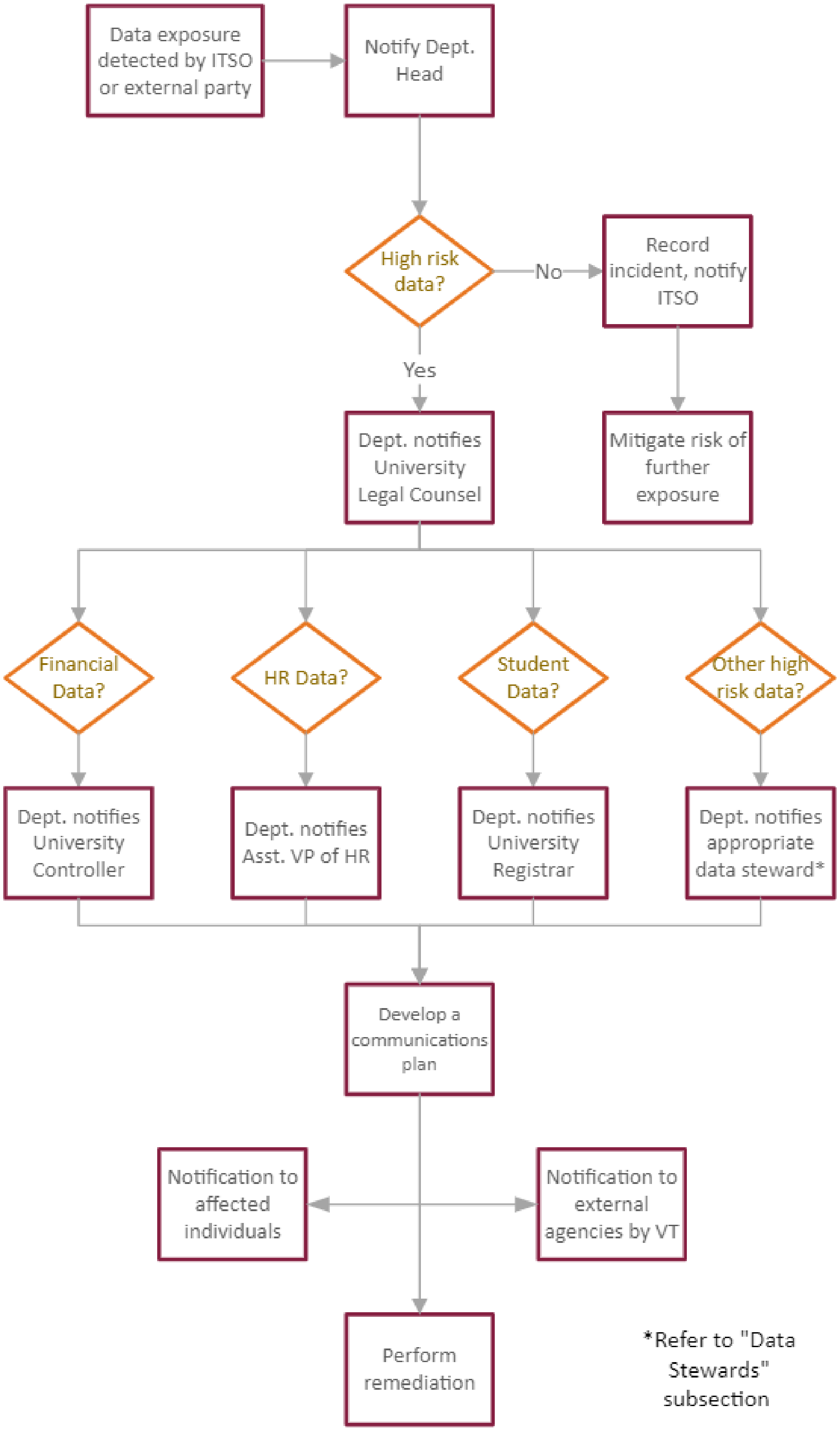
The follow-up report should be shared with the VP for Information Technology and CIO as well as other stakeholders deemed appropriate. A “**Lessons Learned**” meeting with all those involved in the handling and response of the incident should be held and is mandatory for enterprise level incidents.

Appendix A: VT Cyber Incident Response Team Organizational Chart

CIRT Organization Chart



Appendix B: Sensitive Data Response Procedure


Data exposure detected by ITSO or external party
Notify Dept. Head
High risk data?
No
Record incident, notify ITSO
Mitigate risk of further exposure
Yes
Dept. notifies University Legal Counsel
Financial Data?
HR Data?
Student Data?
Other high risk data?
Dept. notifies University Controller
Dept. notifies Asst. VP of HR
Dept. notifies University Registrar
Dept. notifies appropriate data steward*
Develop a communications plan
Notification to affected individuals
Notification to external agencies by VT
Perform remediation

*Refer to "Data Stewards" subsection

Appendix C: CIRT Team Member List and Contact Information

Points of Contact

VA Tech Campus Police: 540-231-6411, Emergency: 911.Chief William (Mac) Babb, Deputy Chief Tony Haga are the most frequent contacts at this office. ***Note: If the violation is deemed to be illegal or life threatening, contact the police first. They will take over the investigation and the CIRT will simply provide whatever information they need for the investigation***.

Appendix D: SENSITIVE DATA NOTIFICATION

Policy 7000, Acceptable Use and Administration of Computer and Communications Systems, section 3.3 states "*Any suspected cybersecurity incident or data exposure must be immediately reported to the appropriate Dean, Director, or Department Head and to the Information Technology Security Office (ITSO).*" The Information Technology Security Officer (ITSO), in consultation with the Office of the General Counsel and appropriate data trustees/stewards, is responsible for determining whether a breach of information security or University private data has occurred and whether notification to affected individuals is required. The ITSO may also seek advice from other key administrators responsible for security and privacy at the University and consult with responsible administrators in the affected campus, area, or unit.

Virginia Tech is required to notify external agencies of an event involving certain data types.

- **FERPA** – all confirmed or suspected breaches of FERPA data must be reported immediately to the US Department of Education. **The ITSO will notify the US Dept. of ED and will be the primary contact with their cybersecurity group.** "The Student Aid Internet Gateway (SAIG) Agreement requires that as a condition of continued participation in the federal student aid programs, PSIs report actual data breaches, as well as suspected data breaches. Title IV PSIs must report on the day that a data breach is detected or even suspected. The U.S. Department of Education (the Department) has the authority to fine institutions—up to $54,789 per violation per 34 C.F.R. § 36.2—that do not comply with the requirement to self-report data breaches. The Department has reminded all institutions of this requirement through Dear Colleague Letters (GEN 15-18, GEN 16-12), electronic announcements, and the annual FSA Handbook." (https://askregs.nasfaa.org/uploads/resources/ED_Cybersecurity_FAQ.pdf#:~:text=The%20Department%20has%20reminded%20all,email%20cpssaig%40ed.gov)
    - To report a breach, ITSO will email cpssaig@ed.gov. The email should include:
        - date of the breach (known or suspected),
        - Impact of the breach (number of records, number of students, etc.),
        - method of the breach (hack, accidental disclosure, etc.),
        - information security program point of contact (email address and phone number are required),
        - remediation status (complete, in-process, etc. with detail), and
        - next steps (as needed). If ITSO cannot email, ITSO should call the Department's security operations center (EDSOC) at 202-245-6550 to report the data listed above. EDSOC operates 24 hours a day, seven days per week.
- **HIPAA** - Details on the HIPAA notification requirements are available here

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

  - When operating under a Business Associate Agreement (BAA) with data provide to VT by a covered entity, VT must notify the covered entity **without unreasonable delay, and no later than 60 days from the discovery of the breach**. The Privacy and Research Data Protection officer will coordinate with the Principal Investigator of the research project to notify the covered entity.

- PCI
  - If your department is an authorized PCI merchant, a PCI data breach notification may need to be done. Contact Becky Ford, paymentcards@vt.edu, 540-231-4543 within 24 hours of discovery of the breach.

Summary

In the scope of research, Virginia Tech is only bound to the requirements of HIPAA data protections when we receive covered data under a Business Associate Agreement (BAA) from a covered entity. In the case of an unauthorized disclosure of unsecured (unencrypted) HIPAA covered data, our obligation is to notify the covered entity “without unreasonable delay and no later than 60 days from discovery of the breach.” Exfiltration of appropriately encrypted data **does not** constitute a data exposure under HIPAA. If Virginia Tech ever becomes a covered or hybrid entity, there will be additional requirements.

These individuals are responsible for notifying the appropriate external agency. Data Trustee/Data Steward contact information: https://it.vt.edu/resources/policies/adms.html .

- Rebecca Folmar, rfolmar@vt.edu, 540-231-7439, Dir. Risk Management. Contacts VT Cyber Insurance Notification must be done once the President authorizes invoking cyber insurance response.
- Randy Marchany, itso@vt.edu, 540-231-6020, CISO, Contacts US Dept of Education. Notifications must be made within 24-72 hours of discovery of an incident involving student (former, current, alumni) data.
- Kay Heidbreder, heidbred@vt.edu, 540-231-6293, 540-953-2054, Univ. Legal Counsel, Contacts VA State Attorney General Office
- Rick Sparks, rasparks@vt.edu, 540-231-7951, University Registrar, FERPA contact
- Trudy Riley, ospdirector@vt.edu , AVP of Sponsored Programs, Office of Research and Innovation, needs to review research project contract/agreement notification requirements
- Julie Cook, prdp@vt.edu, Director of PRDP, HIPAA Research data
- VITA, VA Fusion Center, https://reportcyber.virginia.gov , any of the above incidents need to be reported by the ITSO **within 24 hours of discovery**.

DATA TYPE	NOTIFICATION WINDOW	CONTACT PERSON	DETAILS
FERPA data	ASAP	Randy Marchany itso@vt.edu 540-231-6020	Must notify US Dept of Education
PCI	24 hours	Becky Ford, paymentcards@vt.edu 540-231-4543 Lauren Lawson, lwolfe@vt.edu, 540-231-6277	Must notify Credit Card companies
PII data	72 hours	Kay Heidbreder, heidbred@vt.edu, 540-231-6293	Must notify State Attorney General
Export Controlled	ASAP	OESRC, oesrc@vt.edu	Must notify appropriate Fed Agencies

		540-231-6583	
Sponsored Project Data	ASAP	Trudy Riley, ospdirector@vt.edu	Align with contract requirements
Virginia Fusion Center (VITA)	24 hours	ITSO, itso@vt.edu	Must report any confirmed incident to VITA
HIPAA		Julie Cook, prdp@vt.edu	Within 60 days in general. See below for details

Appendix E: Checklist of major steps for Incident Response and Handling

	Action	Completed
	Detection and Analysis Phase	
1	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling of the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations.	
	Containment, Eradication and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	

8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Source: NIST Special Publication 800-61 revision 2

What to Report

A cyber incident should be reported if it resulted in either:

- Exposure of legally protected data in University databases, such as financial information protected by GLBA,
- Health information protected by HIPAA.

  AND/OR

- Major disruption to normal agency activities carried out via the University’s data communications, such as network unavailability for all or significant portions of an agency due to a denial of service (DoS) attack.

You should report events that have a real impact on your organization. An IT security incident includes, but is not limited to the following events regardless of platform or computer environment, when:

a. Damage is done
b. Loss occurs
c. Malicious code is implanted
d. There is evidence of tampering with data
e. Unauthorized access has been gained or repeated attempts at unauthorized access have been made (from either internal or external sources)
f. There has been a threat or harassment via an electronic medium (internal or external)
g. Access is achieved by the intruder
h. Web pages are defaced
i. A user detects something noteworthy or unusual (a new traffic pattern, new type of malicious code, a specific IP as the source of persistent attacks)
j. There is a denial of service attack on the agency
k. Virus attacks adversely affect servers or multiple workstations
l. Other information technology security incidents occur that could undermine confidence and trust in the Commonwealth's Information Technology systems

UNIX/LINUX Checklist

This section is intended to provide guidance during the examination of a compromised system. Additional steps may be needed to examine a system. Please consult the IT Security Office before performing steps.

☐ Regain control of the system. Some options include disconnecting the system from the network and making an image copy of the system disk(s).

☐ Analyze the intrusion.

☐ Look for modifications made to system software and configuration files.

☐ Look for modifications to data.

☐ Look for tools and data left behind by the intruder.

☐ Review log files.

☐ Look for signs of a network sniffer.

☐ Check other systems on the local network.

☐ Check for systems affected on other local subnets or remote sites.

☐ Recover from the intrusion.

☐ Install a clean version of the OS on the affected system.

☐ Disable unnecessary services.

☐ Install all vendor security patches.

☐ Change all passwords.

☐ Improve the security of your system and network.

☐ Review the Center for Internet Security benchmark documents and the CERT.ORG Unix configuration guidelines checklist.

☐ Install security tools.

☐ Enable maximal logging.

☐ Install software firewall tools.

☐ Reconnect to the network.

Windows Checklist

This section is intended to provide guidance during the examination of a compromised system. Additional steps may be needed to examine a system. Please consult the IT Security Office before performing steps.

☐ Examine log and event files.

☐ Check for odd user accounts and groups.

☐ Look for incorrect group memberships.

☐ Look for incorrect user rights.

☐ Check for unauthorized applications starting at boot.

☐ Check system binaries with something like Tripwire.

☐ Check network configuration and activity.

☐ Check for unauthorized shares.

☐ Examine jobs run by the scheduler service.

☐ Check for unauthorized processes.

☐ Look for unusual or hidden files.

☐ Check for altered permissions on files or registry keys.

☐ Check for changes in user of computer policies.

☐ Make sure the system has not been moved to a different Workgroup or Domain.

☐ Examine all other related systems.

Appendix F: Compromise Questionnaire and Information Gathering

It is important to gather and record information during an incident. This helps with planning and assigning resources. Analysis of gathered information is also important to the incident closure process. The following questions are intended as an example to help with information gathering. Depending on the nature of the incident, it may be appropriate for additional questions to be considered. ***Consult Appendix H before proceeding.***

Information Needed about Detection

1. What is the infection/intrusion type?
2. What time was the incident detected?
3. How was the infection detected?
4. Who detected the infection?
5. What is the incident machine IP address and DNS name?
6. Who is the IT Support for the incident machine?
7. Was a 4Help Ticket created?
    a. What is the ticket number?
8. What time was the initial notification sent?
9. Was network access disabled?
10. Were people contacted? If so, who?

Information Needed from the User

1. Gather user's contact information. User (name, email, phone #)
2. What is the user's job function?
3. What is the primary function of this department?
    a. Who is the user's manager / direct-report?
4. Does the user work with sensitive or covered PII data?
    a. If yes, what types of sensitive or covered PII data?
5. How much sensitive data? (# of files, GBs?, file types, location)
6. What files did the user access during the time of the incident?
7. Did user work with research data?
    a. If so, what types of research data?
8. How much research data (# of files, size?, file types, location)
9. Does the user use university or departmental enterprise systems?
    a. If so, what level of access does the user have?
10. Does the user have access to shared network storage?
11. Are the shared drives automatically mounted?

12. Who else shares the data in those folders?
13. Did the user use encryption on files? If so, what kind(s) of encryption and where are the keys? ITSO may require access to encryption keys.

Questions about the Infection

1. What was the user doing during the incident?
2. Did the user notice any strange things about the computer around that time?
3. Did the user receive any strange emails, or open any unknown attachments?
4. Did the user enter credentials (username, password) on any sites?
5. Did the user install any software?
6. Did the user receive any software updates?
7. Did the user's antivirus software complain or alert?
8. Did the user notice a change in computer performance?
9. Did the user receive any strange Instant Messages?
10. Does the user use their computer for non-work related functions?
11. If so, what function(s)?
12. Facebook/social media? Internet Radio? Email? Online Banking?

Information Needed from Departmental IT Support

1. IT Support contact information (name, email, phone #)
2. Do they have shared drives?
3. Who has access to these drives?
4. What type of data is accessed or used by the system? FERPA, GLBA, University PII, etc.
5. Are they automatically mounted?
6. What types of security precautions have you placed on the system? (AV, Malware Bytes)
7. Is administrative access granted to the user?
8. What types of encryption are used?

Infection Details and Analysis

1. IT person (name, email, phone #)
2. Do they have shared drives?
3. Who has access to these drives?
4. Types of data (see above)
5. Are they automatically mounted?

6. What types of security precautions have been placed on the system?
7. What type of anti-virus is used?
8. Does the user have administrative access?
9. Is there file-based encryption? (think: TrueCrypt)
    a. What type of encryption?

Incident Analysis

1. When was the first sign of an infection?
2. Was this sign indicative of the initial infection?
3. What is the confidence level of the initial infection notice?
4. Is a copy of the malware package available?
5. How long was the machine online after the first sign of an infection?
6. How long before the IT staff was notified?
7. How many Command & Control (C&C) servers are involved?
8. Where are they located?
9. How much data went to each C&C server?
10. Are other devices on the network communicating with these C&C servers?
11. How much data was transferred between the time of the believed initial infection and when the device was pulled off the network?
12. Who were the top talkers?
13. Are they legitimate top talkers?
14. What other network security alerts were triggered by the device?
15. How much traffic remains for the incident period after the top talkers are removed?

Appendix G: Communications Tracking Worksheet

This worksheet is intended to help formulate a communication strategy to share information while containing, eradicating, and recovering from a cyber-incident. **All communications regarding cyber incidents must be conducted through channels that are known to be unaffected by the cyber incident under investigation.**

Note: ***Consult University Legal Counsel and University Relations before communicating with external stakeholders.***

1. **List of possible stakeholders**

   □ VP and CIO for Information Technology
   □ IT Security Office Staff
   □ CIRT Team Members
   □ Departmental Management
   □ Departmental IT Staff
   □ University Legal Counsel Others:
   □ Faculty and Staff
   □ Students
   □ Law Enforcement Agencies
   □ Virginia Tech's technical support community
   □ Outside agencies
   □ Vendors

____

____

____

2. **List those authorized to communicate (limits of authorization)**

3. **List internal communications channels**

   □ Email
   □ Listserv (can be event specific)
   □ Phone/video conferences
   □ Meetings Others:
   □ Office phones
   □ Cell phones

____

____

____

4. **List external communications channels**

   □ Email
   □ Web, Blogs
   □ Listserv (can be event specific)
   □ Phone/video conferences
   □ Meetings Others:
   □ Office phones
   □ Cell phones

____

____

____

5. **Schedule of communications (Discuss appropriate frequency of communications)**

Appendix H: Notification of Outside Organizations Involved in a Cyber Incident

It may be necessary to contact an outside organization to let them know that a machine under their control may be having a negative impact on Virginia Tech's IT systems and networks. The steps provided below are intended to guide communication.

1. Determine technical and administrative contacts of the source machine.
2. Determine WHOIS contact for upstream provider, if one exists.
3. Determine if a US-CERT or "abuse" email address exists if the source machine is from a foreign country.
4. Contact itso-g@vt.edu to see if other campus sites have been attacked/scanned by the source machine.
5. Send a concise email to the WHOIS contact of the source machines. Include:
   - The source site's US-CERT
   - Copy for IT Security Office
   - Copy affected department(s) and personnel.
   - Log excerpts in text of e-mail. **Do NOT send attachments or HTML.**

Appendix I: Internal Audit Guidelines for reporting unacceptable computer use.

Prohibited Activities

University policy 7000 “Acceptable Use and Administrations of Computer and Communications Systems, specifically prohibits use of university resources for personal gain and any other illegal act. Various state laws and standards specifically prohibit downloading, viewing or storing sexually explicit material.

DO:

- Your job! It is always acceptable for employees to perform their duties.
- STOP investigating further once department personnel become aware of situations that may need further review by central offices.
- CONTACT Office of Audit, Risk, Compliance (OARC) and the IT security Office before proceeding. This helps ensure consistent handling of similar situations across the university, preventing unfair treatment and reducing the possibility of lawsuits against the university and its employees.
- Remember it is not your fault that someone in your department has potentially violated state law and university policies and you are doing your duty when reporting to central offices.

DON’T:

- Conduct your own investigation! Other university personnel have undergone extensive computer forensic training.
- Allow deletion of the questionable material. If need be, isolate the machines until further review can be performed.
- Interview the personnel that may be involved until after contacting OARC and the IT Security Office. This will allow for a complete uniform investigation or review (if needed).
- Share the details of the investigation among the department beyond requisite management personnel. There is always the possibility that there is no violation of laws and university policies.

Information to be gathered in the event of an incident:

- The 5W’s: Who, What, When, Where, Why of the incident.
- Example: Steve Jones, IT support staff, discovered potentially inappropriate material when reviewing the reasons for Joan Stevens’ machine slow-down. This review happened in Room 238 of University Hall at approximately 1500 on May 17, 2021. The material in question appeared to be if a sexually explicit nature. The machine has been stored in a locked office.

Applicable Laws and Standards

- Section 2.2-2827 of the Code of Virginia prohibits employees from using an agency-owned or agency leased computer to access, download, print or store sexually explicit content.

Appendix J: University Policies and Standards

- Available at http://www.policies.vt.edu
- Virginia Tech Statement of Business Conduct Standards – http://www.cafm.vt.edu/busprac/business_conduct_standards.php
- 1060 – Policy on Social Security Numbers
- 2000 – Management of University Records
- 2001 – Retention and Storage of Presidential Records
- 2010 – Release of Names and Addresses of Students
- 4082 – Appropriate Use of Electronic Personnel and Payroll Records
- 7000 – Acceptable Use of Computer and Communication Systems
- 7010 – Policy for Securing Technology Resources and Services
- 7025 – Safeguarding Nonpublic Customer Information
- 7030 – Policy on Privacy Statements on Virginia Tech Web Sites
- 7035 – Privacy Policy for Employees' Electronic Communications
- 7040 – Personal Credentials for Enterprise Electronic Services
- 7100 – Administrative Data Management and Access Policy
- Standard for Administrative Data Management http://www.it.vt.edu/publications/pdf/interim_updates/AdministrativeDataManagementStandard2013Nov4signed.pdf
- 7200 – University IT Security Program
- 7205 – IT Infrastructure, Architecture, and Ongoing Operations
- 7210 – IT Project Management
- 7215 – IT Accessibility

Virginia Legislation

- Commonwealth of VA Policy 1.75 – Use of Internet and Electronic Communication Systems
- Code of Virginia 2.2-603.G Incident Reporting Requirement, www.vita.virginia.gov/security/incident/guidance.cfm
- Code of Virginia 18.2-186.6 Data Breach Notification Requirement
- Code of Virginia 2.2-3801 Definitions
- Code of Virginia 2.2-3806 Rights of Data Subjects

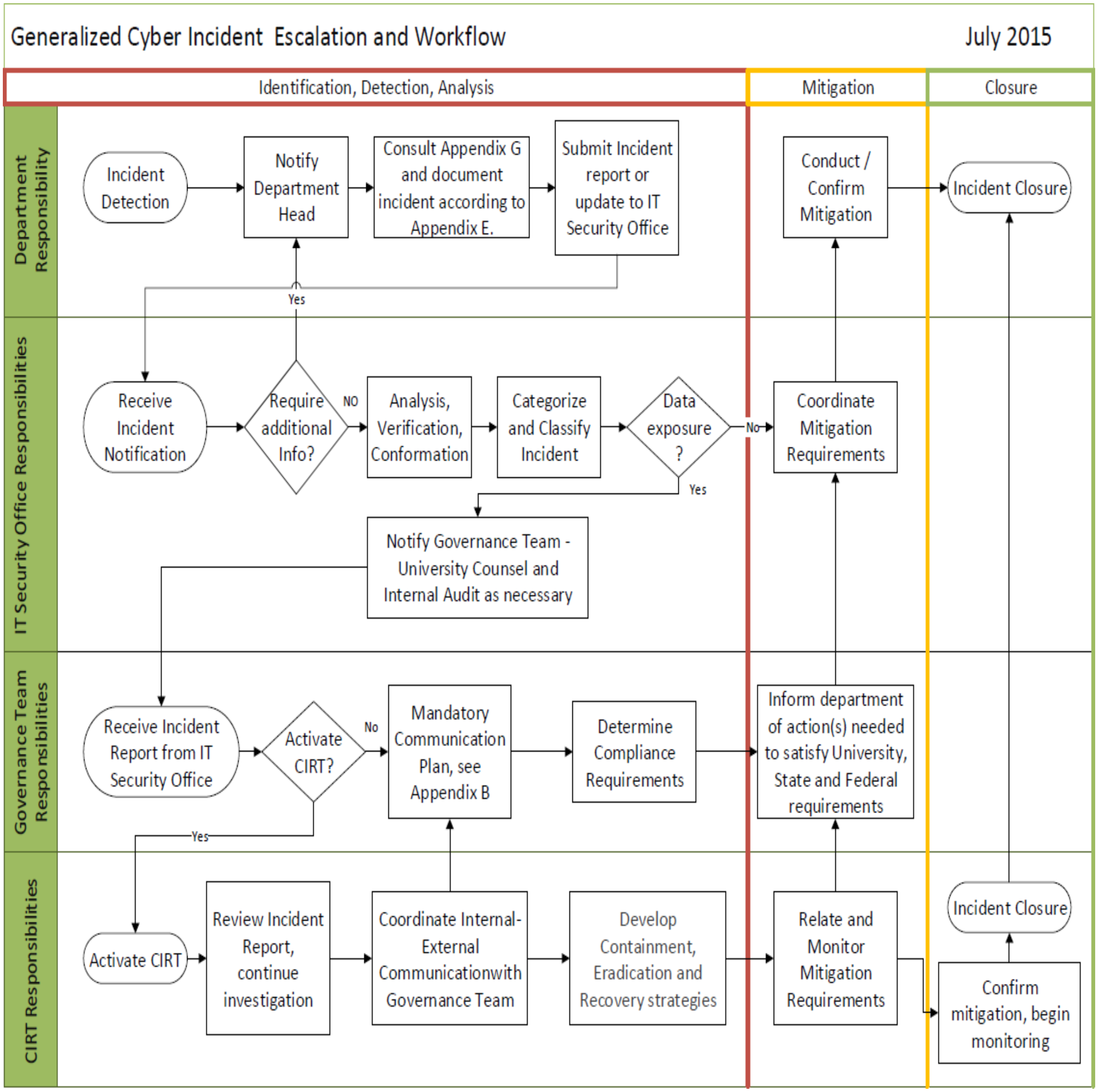
References

Board of Visitor Information Technology Security and Authority Resolution, June 2007, http://www.bov.vt.edu/minutes/07-06-04minutes/attach_v_070604.pdf

Appendix K - Contact information for local police

Virginia Tech Police (540-231-6411)
Blacksburg Police (540-961-1150)
Christiansburg Police (540-382-3131)
Radford Police (540-731-3624)

Appendix L: Generalized Cyber Incident Escalation and Workflow Diagram


Generalized Cyber Incident Escalation and Workflow
July 2015
Identification, Detection, Analysis
Mitigation
Closure
Department Responsibility
IT Security Office Responsibilities
Governance Team Responsibilities
CIRT Responsibilities
Incident Detection
Notify Department Head
Consult Appendix G and document incident according to Appendix E.
Submit Incident report or update to IT Security Office
Conduct / Confirm Mitigation
Incident Closure
Yes
Receive Incident Notification
Require additional Info?
NO
Analysis, Verification, Conformation
Categorize and Classify Incident
Data exposure ?
No
Coordinate Mitigation Requirements
Yes
Notify Governance Team - University Counsel and Internal Audit as necessary
Receive Incident Report from IT Security Office
Activate CIRT?
No
Mandatory Communication Plan, see Appendix B
Determine Compliance Requirements
Inform department of action(s) needed to satisfy University, State and Federal requirements
Yes
Activate CIRT
Review Incident Report, continue investigation
Coordinate Internal-External Communicationwith Governance Team
Develop Containment, Eradication and Recovery strategies
Relate and Monitor Mitigation Requirements
Incident Closure
Confirm mitigation, begin monitoring

Appendix M: Acronyms

CIO:	Chief Information Officer
CIRT:	Computer Incident Response Team
CISO:	Chief Information Security Officer
COV:	Commonwealth of Virginia
CSRM:	Commonwealth Security and Risk Management
DDoS:	Distributed Denial of Service
ES:	Enterprise Systems
FERPA:	Family Educational Rights and Privacy Act
GLBA:	Gramm-Leach-Bliley Act
GDPR:	General Data Protection Regulation (EU)
HIPAA:	Health Insurance Portability and Accountability Act
IDS:	Intrusion Detection System
IMS:	Identity Management Services
IPS:	Intrusion Prevention System
IRM:	Incident Response Manager
ISO:	Information Security Officer
IT:	Information Technology
ITSO:	IT Security Office or IT Security Officer depending on the context
ITAR:	International Traffic in Arms Regulations
ITRM:	Information Technology Resource Management
ITSO:	Information Technology Security Officer
NI&S:	Network Infrastructure and Services
NIST:	National Institute of Standards and Technology
PCI-DSS:	Payment Card Industry Data Security Standard
PII:	Personally Identifiable Information
PIRN:	Personal information requiring notification
SEC501:	Information Security Standard 501
SETI:	Secure Enterprise Technology Initiatives
VCCC:	VITA Customer Care Center
URL:	Universal Resource Locator
US-CERT:	United States Computer Emergency Readiness Team
VITA:	Virginia Information Technologies Agency
VT:	Virginia Tech

INCIDENT An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Also known as "computer security incident", "cyber security incident", "cyber attack". Reference: https://csrc.nist.gov/glossary/term/incident

Record of Changes

Version #	Implemented By	Revision Date	Approved By	Approval Date	***Reason***
4.0	Randy Marchany	03/14/2014	Randy Marchany		*Reformat plan, improve process documentation, update team members, update version number*
4.1	Randy Marchany	07/27/2014	Randy Marchany		*Update documentation, expand remaining sections.*
4.2	Randy Marchany	8/1/2014	Randy Marchany		*Updating diagrams*
4.3	Brad Tilley	11/3/2014			*Minor corrections and clarifications*
4.4	Brenda van Gelder	4/1/2015			*Incorporate line managers feedback provided to date*
4.5a	Randy Marchany	6/1/2015			*Incorporate changes, update diagrams*
4.6	Angela Correa	6/16/2015			*Grammar and continuity edit*
4.7	Jean Plymale	06/30/2015			*Add Internal Audit guidelines, acronyms, contact info for local police and update document structure to reflect these changes and additions.*
4.8	Angela Correa	7/9/2015			*Integration of 2015 edits.*
4.9	David Raymond	11/18/2015	Randy Marchany	11/18/2015	*Final edits.*
5.0	David Raymond	1/28/2016	Randy Marchany	1/28/2016	*- Updated Org Chart (App. A)* *- Finalized Version*
5.1	Randy Marchany	4/12/2022			*- Updating entire document to 2022 standards. Updated Appendix C with current contact info. Updated all web and document links.*
5.2	Randy Marchany	7/12/2022			*- Added definition of "GDPR" and "incident" to Appendix L*
5.3	Randy Marchany	8/3/2022			*- Added VITA incident notification info to Appendix C*
5.4	Randy Marchany	1/24/2023			*- updated ITSO office number, updated TOC, created Appendix D for notifications, adjusted other appendices*

					-
					-
					-
					-
					-
					-
					-
					-
					-
					-
					-
					-
					-
					-
					-
					-