Virginia Tech

Incident Response Manual

V6.0 | October 30, 2026

PURPOSE

This manual establishes Virginia Tech's coordinated response framework for cybersecurity incidents and major technology outages, including third-party provider outages and breaches.

Important: If an incident is deemed illegal or life-threatening, contact Virginia Tech Police at 540-231-6411 or Emergency: 911.

Information Technology Security Office (ITSO)
Email: itso-g@vt.edu | Phone: 540-231-6020

IT Security Incident Quick Guide

REPORT IMMEDIATELY

Call 4HELP immediately at (540) 231-4357 (24x7) if you suspect or become aware of:

- A cybersecurity incident involving high-risk data, compromise, ransomware, phishing, or targeted activity.
- Incidents with potential for severe financial, reputational, legal or regulatory impact
- A critical system disruption, material degradation, or outage with enterprise-wide or multi-unit impact.
- A suspected or confirmed outage or breach involving a third-party provider.
- An event that may create significant operational, legal, regulatory, reputational, public, or media impact.

For threats to life or property, call 911 immediately.

NON-URGENT REPORTING

Report non-urgent security events through the ITSO website: https://security.vt.edu/incident

Non-Urgent

- Does not involve high-risk data.
- Does not involve ransomware, a confirmed compromise, or active phishing/targeted attacks.
- Has limited impact to a single user, device, or department.
- Is not causing a critical outage or significant degradation of service.
- Does not create significant legal, regulatory, financial, reputational, media, or operational risk.
- Does not involve a third-party provider breach or outage.

INFORMATION TO PROVIDE

- Your unit's security or operational point of contact.
- Observed symptoms, scope, timing, affected devices/accounts/services, and business impact.
- Whether a third-party provider, integration, API, credential, or sensitive data may be involved.
- Known actions already taken and persons or offices notified.
- Whether the event is ongoing, spreading, or affecting multiple departments.

GENERAL INCIDENT GUIDELINES

- **Remain Calm**
  - Avoid making assumptions or taking unilateral action before the nature and scope of the incident are understood.
  - Premature remediation may impede investigation efforts and increase organizational risk.
- **Preserve Evidence**
  - Maintain the integrity of affected systems and data.
  - Avoid modifying, rebooting, investigating, or otherwise altering impacted assets unless directed by ITSO.
  - Where appropriate, preserve system images, clones, and logs to support forensic analysis.
- **Engage ITSO Immediately**
  - Notify ITSO as soon as a potential incident is identified and provide timely updates as new information becomes available.

  - Early engagement enables coordinated response, accurate risk assessment, and effective containment.
- **Maintain Reliable Communications**
  - If university email, messaging, or telephony services may be compromised, use alternate communication channels to coordinate with ITSO.
- **Limit Information Sharing**
  - Restrict communications to leadership, ITSO, and personnel directly involved in the response.
  - Protect sensitive information and avoid unnecessary distribution while the incident is being assessed.
- **Document Key Actions and Decisions**
  - Maintain a record of significant observations, actions taken, timelines, and decision rationale.
  - Provide documentation to ITSO to support incident response, investigation, and post-incident review.

Security Incident Response Lifecycle

Phase 1: Detection & Assessment \ Immediately Upon Identification

Unit Leadership Responsibilities

- Treat potential security incidents as a priority operational matter.
- Promptly notify the Information Technology Security Office (ITSO) upon discovery or suspicion of an incident.
- Designate an accountable point of contact for incident coordination.
- Collect and provide available information to support initial assessment and severity determination.

What to Expect from ITSO

- Assess incident severity and organizational risk.
- Initiate incident triage and information gathering.
- Establish response priorities and coordination requirements.

Phase 2: Containment & Evidence Preservation \ Within the First 15 Minutes

Unit Leadership Responsibilities

- Preserve affected systems and data in their current state.
- Avoid actions that could alter evidence, disrupt investigations, or increase risk.
- Coordinate with ITSO on containment activities.
- Preserve critical logs, system images, and relevant documentation.
- Communicate potential business impacts, affected services, and leadership concerns.
- Notify appropriate unit leadership and stakeholders.

Actions to Avoid

- Shutting down affected systems unless directed by ITSO.
- Conducting independent investigations or forensic activities.
- Changing system configurations, credentials, or network settings.
- Running diagnostic or remediation tools without coordination.
- Attempting to resolve the issue before scope and impact are understood.

What to Expect from ITSO

- Lead containment and investigative activities.
- Establish and coordinate the incident response strategy.
- Provide guidance on evidence preservation and risk mitigation.

Phase 3: Investigation, Remediation & Recovery \ Days Following Incident Identification

Unit Leadership Responsibilities

- Continue supporting information gathering and documentation efforts.
- Partner with ITSO to assess operational, regulatory, and data-related impacts.
- Assist in developing and executing recovery and remediation plans.
- Escalate significant findings or changes in risk immediately.
- Validate that systems and services are operating as expected following restoration.

What to Expect from ITSO

- Coordinate enterprise incident response activities.
- Deliver ongoing analysis of incident scope, impact, root cause, and timeline.
- Identify additional systems, accounts, or services requiring review.
- Provide regular updates to leadership and stakeholders.
- Develop remediation recommendations and long-term risk-reduction strategies.
- Monitor for residual or recurring threats.

Phase 4: Closure & Continuous Improvement \ Following Incident Resolution

Unit Leadership Responsibilities

- Implement agreed-upon security enhancements and corrective actions.
- Update operational procedures and supporting documentation.
- Incorporate lessons learned into future planning and risk-management activities.

What to Expect from ITSO

- Deliver an executive incident summary and closure report.
- Facilitate post-incident reviews and lessons-learned discussions, as appropriate.
- Recommend strategic security improvements to strengthen resilience and reduce future risk.

Section 1: Introduction

Authority

Oversight of the security of university information technology resources and information is assigned to the Vice President for Information Technology and Chief Information Officer (VPIT-CIO) by the Virginia Tech Board of Visitors. Virginia Tech Policy 7010, "Policy for Securing Technology Resources and Services," provides the Information Technology Security Office (ITSO) authority to respond to threats to university networks, systems, and services.

Purpose and Scope

This manual provides a coordinated framework for detecting, assessing, containing, recovering from, communicating about, and learning from cybersecurity incidents and major technology outages. It applies to university-owned technology, third-party services that host, process, transmit, or access Virginia Tech data, and major internally hosted technology outages.

- It supplements, and does not replace, continuity of operations, disaster recovery, emergency management, legal, regulatory, procurement, or departmental procedures.
- It covers cybersecurity incidents and material technology outages, including third-party outages that do not involve a confirmed security compromise.
- It applies to all university locations, departments, systems, services, integrations, and affected technology stakeholders.

Audience

This manual is for ITSO staff, the Technical Response Team (TRT), system and network administrators, service and business owners, technical support staff, unit leadership, Communications and Marketing, Legal Counsel, Audit, Risk and Compliance, and other personnel responsible for preparing for or responding to incidents and major outages.

Section 2: Mission, Strategy and Goals

Mission

Virginia Tech will coordinate timely, evidence-informed response actions that protect people, university operations, technology services, and university data; restore services safely; meet applicable notification obligations; and reduce the likelihood and impact of future incidents.

1. Limit the impact of cyber incidents and major technology outages while safeguarding the university community.
2. Protect university technology infrastructure, sensitive data, and critical services.
3. Provide consistent incident and outage response, including clear authority for containment, redirection, restoration, and communications.
4. Coordinate effectively with third-party providers, internal service owners, and external response organizations.
5. Restore operations safely and verify recovery before normal service is resumed.
6. Capture lessons learned and implement corrective actions.

Strategy and Goals for Cyber Incident Response

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

The ITSO manages and coordinates the detection, identification, containment, eradication, and recovery of reported cybersecurity incidents in collaboration with Virginia Tech departments and their IT personnel. The CISO or the Deputy Chief Information Security Officer (DCISO), acting as the CISO's standing delegate, is authorized to classify threats as enterprise risks and activate the Virginia Tech Technical Incident Response Team (TRT).

The TRT is activated when a cybersecurity incident requires coordinated technical response beyond routine local incident handling. The TRT is activated when a cybersecurity incident affects University IT systems or services at an enterprise-wide or multi-unit level, including incidents involving multiple departments that require both local and enterprise administrator support.

For enterprise-wide cybersecurity incidents, the Incident Management Team (IMT) is activated when the incident:

- Involves multiple departments and requires local and enterprise administrator support from affected departments
- Has enterprise-wide or multi-unit impact
- Generates significant public or media attention

The CISO serves as Incident Commander for cybersecurity incidents. For a major technology outage that does not involve a cybersecurity incident, the relevant IT service owner leads operational response. For an enterprise-wide outage, the service owner serves as Operational Incident Lead, while the VPIT-CIO retains executive authority for service disablement, user redirection, and restoration.

Section 3: Incident Response and Major Outage Governance

Virginia Tech Technical Response Team (TRT)

The Virginia Tech Technical Response Team (TRT) is the hands-on technical response body. The first reference uses the full name; subsequent references use TRT. The TRT includes ITSO personnel and representatives from relevant technology, identity, networking, enterprise systems, infrastructure, research computing, collaboration, and affected departmental teams. The CISO or the Deputy Chief Information Security Officer (DCISO), as standing delegate, may classify incidents and activate the TRT.

Incident Management Team (IMT)

For enterprise-wide cybersecurity events, executive leadership from across the university is assembled for crisis response and communications. Virginia Tech's Incident Management Team (IMT), directed by Virginia Tech Emergency Management (VTEM), provides executive and cross-functional coordination for enterprise-wide crisis response, including cybersecurity incidents. The IMT is flexible, adaptable, and multi-disciplined representing a significant portion of the university employees by extension. In the case of cybersecurity incident response, the CISO or D/CISO will work with the VTEM Executive Director or their designee to engage appropriate IMT members based on the nature of the incident. Additional personnel beyond the IMT will be added as necessary. VTEM will support coordination and communication among IMT members, but IT security leadership will continue to serve as incident commander. University leaders who might be involved in IR include:

- Vice President for Information Technology and Chief Information Officer (VPIT-CIO)
- Associate Vice President for Security & Identity and Chief Information Security Officer (CISO)
- Deputy CISO
- University Legal Counsel
- University President
- Executive Vice President and Provost
- University Office of Audit, Risk and Compliance (OARC)
- Division of Student Affairs/Student Conduct
- Virginia Tech Police Department
- Procurement Office
- Affected Data Trustees and Data Stewards

IMT Activation

The IMT must be activated when any one of the following conditions exists:

- An enterprise-wide attack involving multiple departments and requiring local and enterprise administrator support from affected departments.
- Enterprise-wide or multi-unit impact.
- Significant public or media attention.

Confirmed or suspected sensitive-data exposure, a critical-service outage, a third-party/provider compromise, or legal/regulatory notification risk does not by itself activate the IMT unless it has enterprise-wide or multi-unit impact. Localized events remain under ITSO/TRT handling and applicable unit processes.

Incident and Operational Leadership

- Cybersecurity incident: the CISO serves as Incident Commander; the DCISO is the standing delegate.
- Major non-security outage: the relevant IT service owner serves as Operational Incident Lead.
- Mixed event (outage and suspected/confirmed compromise): the CISO/Incident Commander leads the overall incident; the service owner leads operational recovery under that command.
- The VPIT-CIO, in consultation with the service owner and IMT when activated, authorizes third-party service disablement, user redirection, and service re-enablement for high-impact services.

Emergency Authority and Communications

Emergency Temporary Actions

When delay would increase harm, the CISO/Incident Commander may direct immediate temporary containment, including disabling integrations, rotating credentials, or redirecting a URL. The CISO must promptly notify the VPIT-CIO and IMT, when activated, for review and ratification, modification, or termination of the action. For an enterprise-wide non-security outage, the Operational Incident Lead may take immediate temporary action, such as redirecting users to an approved status page, when delay would materially worsen the outage; the Operational Incident Lead must promptly notify the VPIT-CIO and IMT.

Reporting and Communications

Cybersecurity incidents and major technology outages may be reported through 4HELP, the ITSO website, email, telephone, in person, or a ServiceNow ticket. All incident communications must use channels known to be unaffected by the incident. Communications and Marketing drafts and coordinates external and enterprise communications. Legal Counsel and the CISO/Incident Commander must approve messages before release.

For third-party incidents, the Incident Commander sets vendor notification and status-update cadence based on incident severity. Communications and Marketing maintains separate current templates for: initial holding message, service outage, suspected vendor breach, confirmed data exposure, service restoration, and extended outage.

Incident Classification

The CISO or DCISO classifies incidents as local or enterprise-wide and determines whether to activate the TRT and IMT. Classification considers scope, impact, affected data, criticality, operational continuity, legal and regulatory implications, and public or media attention.

Incident Classification and Response Matrix

Classification Level	Typical Characteristics	Illustrative Impact / Examples	Response	TRT Activation	IMT Activation
3 — Critical	Enterprise-wide cybersecurity incident; attack against University infrastructure; widespread service disruption; or an event requiring coordinated local and enterprise administrator support across multiple departments.	DDoS attack against University servers; attack on core network infrastructure; large-scale disruption affecting a significant portion of the Virginia Tech community; compromise of an enterprise service or identity platform affecting multiple units.	The CISO or DCISO activates the full Technical Response Team (TRT). ITSO coordinates technical response with affected local IT administrators, service owners, and enterprise teams. The Incident Management Team (IMT) is activated. University leadership, Legal Counsel, Communications and Marketing, Virginia Tech Police, and other stakeholders are engaged as appropriate.	Full TRT — Yes	Yes
2 — High	Affects sensitive data, critical services, privileged accounts, or a defined group of individuals; may involve elevated access or a high-risk third-party service. The event does not yet meet enterprise-wide or multi-unit IMT activation criteria.	Compromise of Banner, Exchange, Active Directory, domain controller, or Learning Management System administrator account; suspected compromise of a third-party provider hosting Virginia Tech data; outage of a critical service affecting one or more units; exposure of sensitive data affecting a defined population.	ITSO coordinates response with the affected service owner and local IT administrators. The CISO or DCISO determines whether to activate a targeted TRT response. Legal Counsel and other relevant stakeholders are engaged when required by the nature of the data, regulatory obligations, or incident scope.	As directed by CISO/DCISO	No, unless enterprise-wide or multi-unit impact, or significant public/media attention
2 — High	Affects a single individual or system but involves a significant amount of sensitive data, elevated access, or material risk to university information.	Compromised faculty or staff device containing university-defined sensitive data; physical theft of a computer containing sensitive data; compromise of a privileged account limited to one unit.	ITSO leads or coordinates the response with the affected unit. Preserve evidence, assess data and account exposure, contain the event, and complete applicable legal, regulatory, and notification processes.	As directed by CISO/DCISO	No, unless enterprise-wide or multi-unit impact, or significant public/media attention
1 — Moderate	Affects data or services for a group of individuals but does not involve sensitive data or elevated privileges.	Compromise of an account with access to a shared folder containing non-sensitive data; localized service disruption affecting a department or work group.	Local IT administrators respond with ITSO notification, event logging, progress monitoring, and technical guidance. ITSO may provide or coordinate forensic support when local capabilities are insufficient.	No, unless escalated by CISO/DCISO	No
1 — Moderate	Affects data or services of a single individual and does not involve sensitive data beyond that individual's own information.	Compromised faculty, staff, or student device with no University-defined sensitive data; isolated account compromise.	Local IT administrators respond with ITSO notification and guidance. Document actions, restore services, and monitor for recurrence.	No, unless escalated by CISO/DCISO	No

0 — Low	Very minor, routine, informational, or undetermined event with no identified material impact.	Network scans; host-based firewall logs; IDS/IPS alerts; routine suspicious activity requiring review.	ITSO records, analyzes, and routes relevant information to central logging or monitoring services. Escalate if additional evidence indicates a broader incident or material impact.	No	No

Classification and Activation Notes

- The CISO or DCISO has authority to classify incidents and activate the TRT.
- A full TRT activation is required when a cybersecurity incident affects University systems or services at an enterprise-wide or multi-unit level, including events requiring local and enterprise administrator support across affected departments.
- The IMT is activated only when an event:
    - involves multiple departments and requires local and enterprise administrator support;
    - has enterprise-wide or multi-unit impact; or
    - generates significant public or media attention.
- Confirmed or suspected sensitive-data exposure, a critical-service outage, a third-party compromise, or legal/regulatory notification risk does not independently require IMT activation unless the event meets the enterprise-wide, multi-unit, or significant public/media-attention criteria.
- The CISO may direct immediate temporary containment when delay would increase harm. This may include disabling integrations, rotating credentials, or redirecting users to an approved status or alternate page, followed by prompt notification to the VPIT-CIO and IMT when activated.

Virginia Tech Incident Response RACI Matrix

Activity	ITSO / TRT	Service Owner / Local IT	IMT	Communications	Legal / Compliance	VPIT-CIO
Detection, reporting & triage	A/R	R	I	I	C	I
Classification & activation	A/R	C	I	I	C	I
Containment & preservation	A/R	R	I	I	C	I
Third-party outage/breach response	A/R for assessment and cyber containment	R for service, vendor coordination, recovery	C / I when activated	R for approved messaging	C	A for disablement, redirection, re-enablement
Recovery & restoration	C / R for security validation	R	I	C	C	A for high-impact authorization
Notifications & communications	C	C	I	R	A for legal/regulatory content	A for enterprise executive messaging
Closure & lessons learned	A/R	R	C	C	C	I

Legend: R = Responsible; A = Accountable; C = Consulted; I = Informed.

Section 4: Response Process

Stage 1: Detection and Classification

Immediately report events to 4HELP or ITSO. The CISO or DCISO classifies the event, activates the TRT as appropriate, and determines whether IMT activation criteria are met.

TRT / ITSO	Affected Unit / Service Owner
• Establish initial scope, impact, affected services, data, and stakeholders. • Identify whether the event is cybersecurity, operational, or mixed. • Begin the incident record and preserve available evidence. • Make external notifications in coordination with legal counsel's office and appropriate data stewards	• Prioritize response; provide relevant records, contacts, and business impact information.

Stage 2: Containment and Preservation

Containment actions are selected to limit further harm while preserving the ability to investigate and recover.

TRT / ITSO	Affected Unit / Service Owner
• Direct technical containment; preserve relevant logs and configurations; coordinate credential, account, and integration actions. • For third-party compromise, request provider evidence preservation where permitted by contract and provider capabilities.	• Determine data elements that might be exposed and notify incident commander • Do not independently modify or investigate affected systems unless directed. Preserve logs and document actions.

Stage 3: Analysis, Eradication and Recovery

The TRT and affected service owners assess root cause, exposure, operational impact, recovery options, and residual risk.

TRT / ITSO	Affected Unit / Service Owner
• Validate remediation and recovery conditions. • Coordinate with the provider and affected units. • Confirm systems, integrations, and credentials are safe to restore.	• Develop and execute continuity or workaround procedures; report new information promptly.

Stage 4: Closure and Follow-up

Close the event only after recovery is validated, notifications are complete, and required follow-up actions have owners and due dates.

TRT / ITSO	Affected Unit
• Prepare closure documentation and, when required, lead a post-incident review. • Track corrective actions to completion.	• Update local documentation and participate in lessons learned.

Appendices

Appendices have been renumbered following removal of the prior organizational-chart appendix. Flowcharts and workflow language have been updated to use IMT and TRT terminology.

Appendix A: Role-to-contact reference for incident response coordination

Purpose. This reference maps the roles shown in the CIRT organizational diagram to publicly listed Virginia Tech contacts. Team-based functions should be maintained through distribution lists, duty contacts, or separate internal rosters.

1. Primary Leadership Contacts

Diagram Role	Primary Contact	Contact Information
Information Redacted ITSO holds unredacted document		

2. Supporting Offices and Functions

Function	Primary or Alternate Contact	Contact Information
Information Redacted ITSO holds unredacted document		

3. Data Trustees and Data Stewards

The appropriate contact depends on the affected data domain. For an information-security incident, the following assignments are the most directly relevant:

Data Responsibility	Contact	Role
Information Redacted ITSO holds unredacted document		

4. Public Source References

Division of IT Leadership: https://it.vt.edu/administration/leadership.html

IT Security Office Staff: https://security.vt.edu/about/staff/

Governance at Virginia Tech: https://governance.vt.edu/

Division of Enterprise Risk and Integrity: https://eri.vt.edu/

University Legal Counsel Contacts: https://ulc.vt.edu/Contact.html

Virginia Tech Police Directory: https://police.vt.edu/about/directory.html

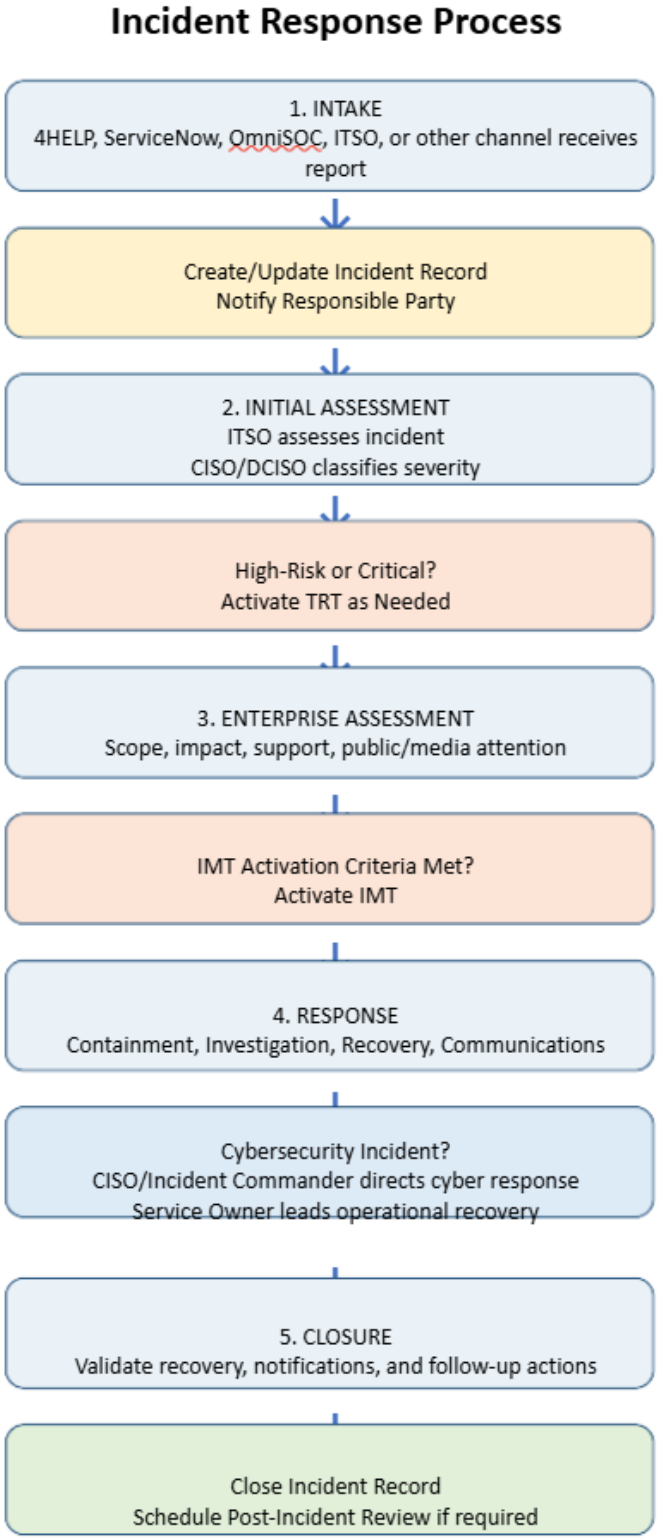
Emergency Management Contact: https://emergency.vt.edu/about/contact.html

Virginia Tech Brand Center Contacts: https://brand.vt.edu/contacts.html

Data Domains and Trustees: https://it.vt.edu/resources/policies/adms/data-domains.html

Data Stewards and Data Areas: https://it.vt.edu/resources/policies/adms/data-stewards.html

Appendix B: Incident Response Workflow

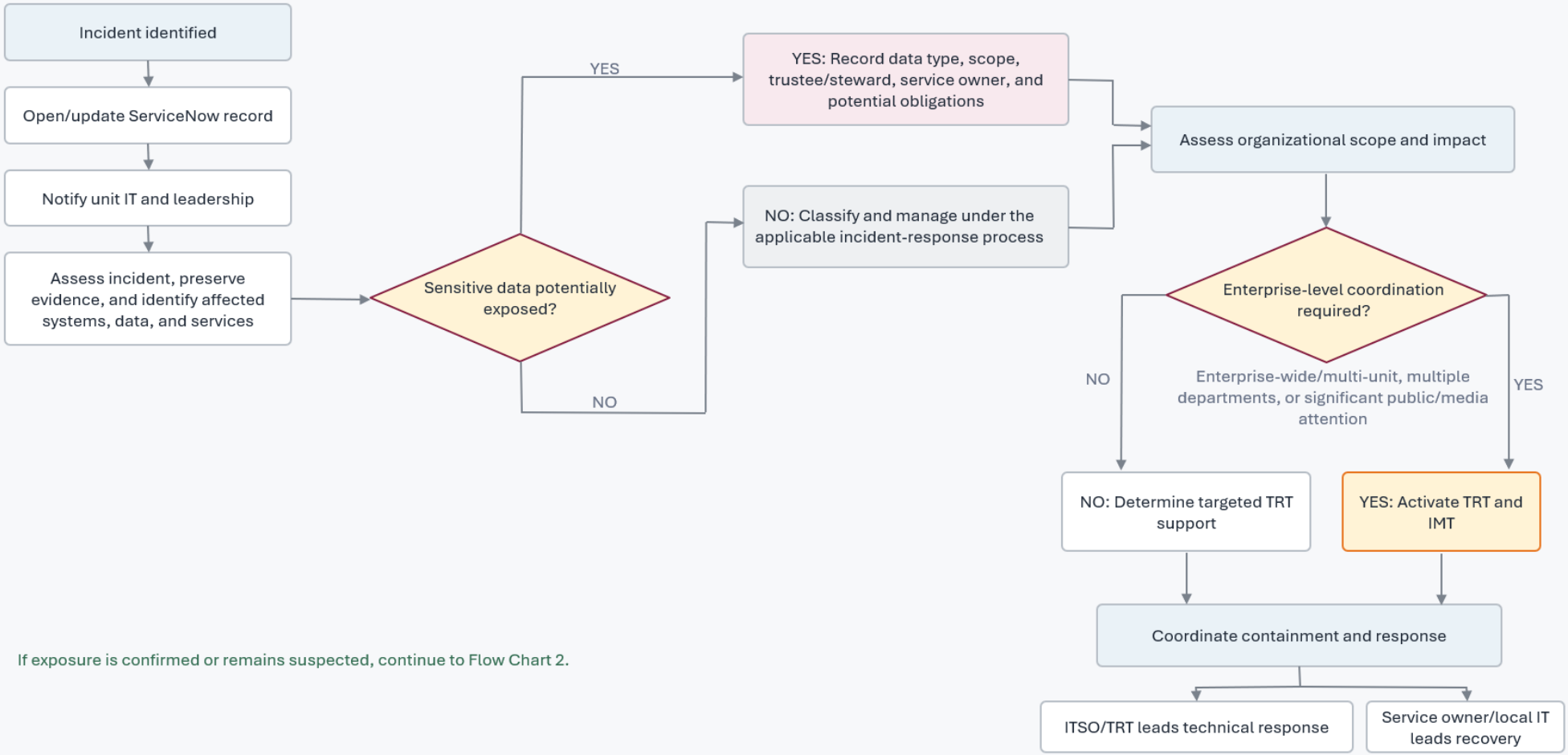


Appendix C: Sensitive Data Response Procedure

Use this procedure when a confirmed or suspected event involves high-risk, restricted, regulated, or otherwise sensitive university data. Notify appropriate department support staff, the applicable data trustee/steward, ITSO, Legal Counsel, and other required parties. Determine notification obligations under FERPA, PCI, research-protected health information, sponsored-project, export-control, and other applicable requirements.

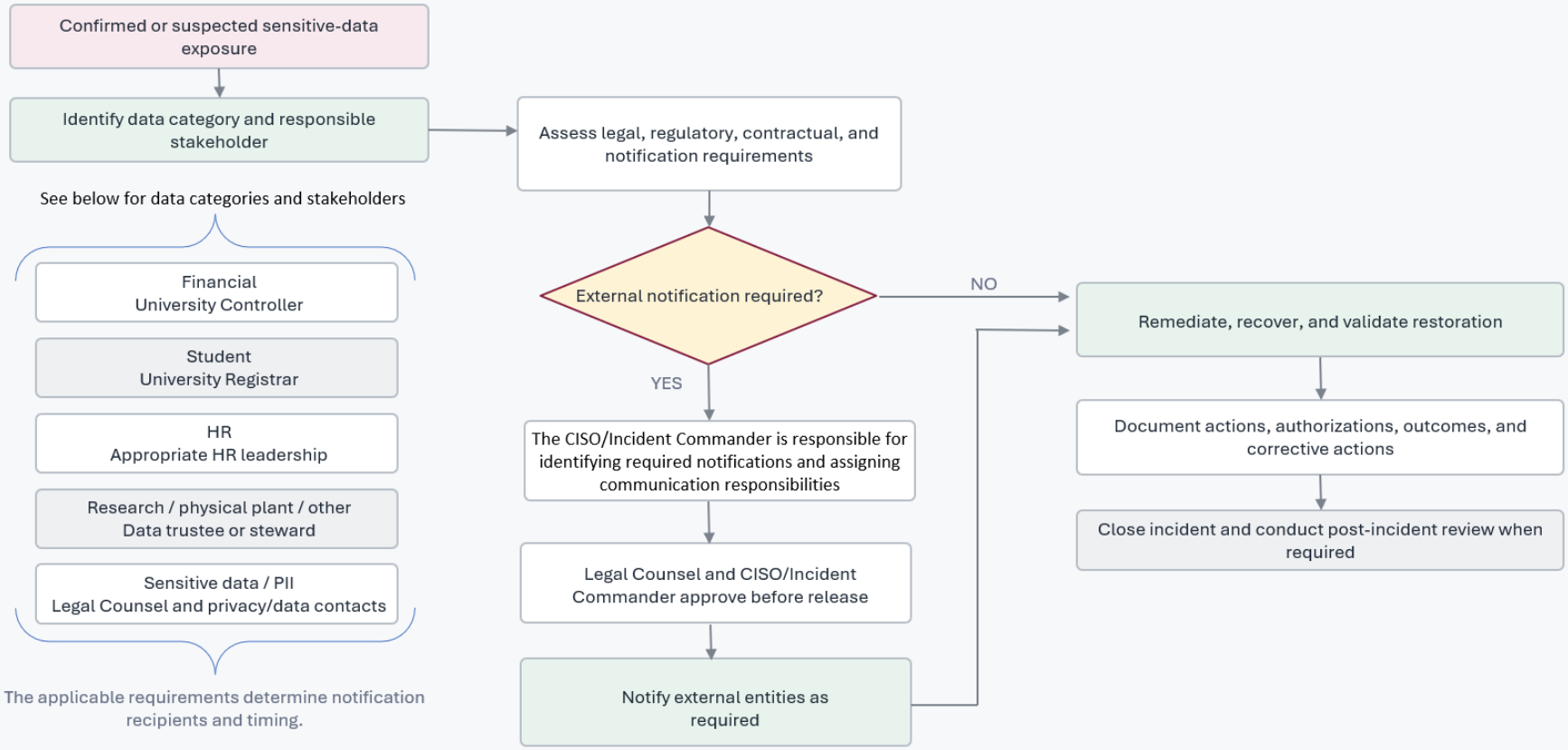
Flow Chart 1: Incident Assessment and Escalation

Use for all cybersecurity incidents. This chart determines response structure and whether Flow Chart 2 applies.



Flow Chart 2: Sensitive Data Obligations and Closure

Use only for confirmed or reasonably suspected sensitive-data exposure.



Appendix D: Sensitive Data Notification

Virginia Tech may be required to notify external agencies when an incident involves certain data types. The Information Technology Security Office (ITSO), applicable data trustee or steward, Legal Counsel, and other responsible offices will coordinate notification requirements based on the data involved, incident scope, applicable law, contractual obligations, and regulatory requirements.

FERPA Data

All confirmed or suspected breaches involving FERPA data must be reported immediately to the U.S. Department of Education. ITSO will notify the U.S. Department of Education and serve as Virginia Tech's primary contact with its cybersecurity group.

The Student Aid Internet Gateway (SAIG) Agreement requires postsecondary institutions participating in federal student-aid programs to report actual and suspected data breaches on the day a breach is detected or suspected. The U.S. Department of Education may impose penalties for failure to meet applicable self-reporting obligations.

To report a breach, ITSO will email FSASchoolCyberSafety@ed.gov. The notification should include:

- Date of the known or suspected breach;
- Impact of the breach, including the number of records, students, or other affected individuals;
- Method of the breach, such as a cyberattack, accidental disclosure, or other event;
- Information security program point of contact, including email address and telephone number;
- Remediation status, including completed and in-progress actions; and
- Planned next steps, as applicable.

If ITSO cannot send an email notification, ITSO should contact the Department's Security Operations Center (EDSOC) at 202-245-6550. EDSOC operates 24 hours a day, seven days a week.

Reference:
https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-02-09/updates-gramm-leach-bliley-act-cybersecurity-requirements

Research Protected Health Information (R-PHI)

For research involving protected health information, Virginia Tech is subject to HIPAA requirements when it receives covered data from a covered entity under a Business Associate Agreement (BAA).

In the event of an unauthorized disclosure of unsecured, unencrypted HIPAA-covered data, Virginia Tech must notify the covered entity without unreasonable delay and no later than 60 days after discovery of the breach. Exfiltration of appropriately encrypted data does not constitute a reportable HIPAA data exposure. If Virginia Tech becomes a covered entity or hybrid entity, additional requirements may apply.

The Privacy and Research Data Protection Officer will coordinate with the Principal Investigator and the covered entity, as applicable, regarding notification.

Payment Card Industry (PCI) Data

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

External Notification Contacts

Data trustees and data stewards are listed at:
https://it.vt.edu/resources/policies/adms.html

Data Type	Notification Window	Responsible Office	Details
FERPA data	Within 24 hours	Information Technology Security Office (ITSO); Office of the University Registrar; Office of University Scholarships and Financial Aid	Must notify the U.S. Department of Education.
PCI	Within 24 hours	Payment Card Compliance Program; Treasury Operations and University Bursar	Must notify applicable credit-card companies.
PII data	Within 72 hours	Office of University Legal Counsel	Must notify the State Attorney General, as required.
Export Controlled	ASAP	Office of Export and Secure Research Compliance (OESRC)	Must notify appropriate federal agencies, as required.
Sponsored Project Data	ASAP	Office of Sponsored Programs (OSP)	Notification and response must align with contract requirements.
Virginia Fusion Center (VITA)	Within 24 hours	Information Technology Security Office (ITSO)	Must report any confirmed incident to VITA.
Research PHI (R-PHI)	Within 60 days of discovery of breach	Privacy and Research Data Protection Program (PRDP)	Notify the Privacy and Research Data Protection Officer as soon as possible.
Cyber Insurance	When needed	Risk Management and Insurance Programs	Contact when a cyber-insurance claim may be required.

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

In some cases, it may be necessary to notify an external organization that a system under its control appears to be adversely affecting Virginia Tech's information systems or network resources. The following guidance is intended to support those communications. The IT Security Office (ITSO) is responsible for contacting external organizations regarding cybersecurity incidents that affect them.

1. Identify the technical and administrative contacts associated with the source system.
2. Determine the WHOIS / RDAP contact information for the upstream service provider, if available.
3. For sources located outside the United States, identify any available US-CERT equivalent or designated abuse reporting email address.
4. Contact **itso-g@vt.edu** to determine whether other university systems have experienced attacks or scanning activity from the same source.
5. Send a concise notification email to the identified WHOIS or abuse contact. The message should:
    - Include the source organization's US-CERT or equivalent contact, if available.
    - Copy the IT Security Office.
    - Copy any affected departments or personnel.
    - Include relevant log excerpts within the body of the email.
    - **Do not send attachments or HTML-formatted messages. Use plain text only.**

Appendix F: University Policies and Standards

Applicable university policies and standards are available through Virginia Tech policy and IT resources. Relevant Virginia law and external standards apply according to the incident, data type, and affected service.

Available at http://www.policies.vt.edu

- All university IT policies and standards are available at https://it.vt.edu/content/it_vt_edu/en/resources/policies.html
- Statement of Business Conduct Standards: http://www.cafm.vt.edu/busprac/business_conduct_standards.php

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

Appendix G: 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 H: Third-Party Outage and Breach Playbook

This playbook applies to all third-party providers that host, process, transmit, or access Virginia Tech data. A third-party outage includes material degradation, disruption, or loss of access to a provider-hosted service, not only complete unavailability.

Quick-Reference Checklist

Phase	Required actions
First hour	Notify ITSO immediately; create/update incident record; determine whether the event is cybersecurity, operational, or mixed; contact provider; identify affected business functions, data, integrations, credentials, vanity URLs, and continuity impacts; preserve VT-side evidence when feasible and directed; assess IMT activation.
Containment	CISO/Incident Commander directs cyber containment. Disable relevant integrations and take temporary protective actions as needed. Rotate or revoke all relevant API keys, administrative credentials, service-account passwords, tokens, and certificates after suspected or confirmed compromise unless the Incident Commander documents a written exception. Redirect vanity URLs to 4help status page.
Communications	Incident Commander sets provider update cadence based on severity. Communications and Marketing uses maintained templates. Legal Counsel and CISO/Incident Commander approve messages before release.
Restoration	Service owner and CISO/Incident Commander confirm required containment, credential rotation, critical-integration review, and applicable vendor assurances before seeking VPIT-CIO authorization to re-enable high-impact service.
Closure	Document owner, time, authorization, action, and outcome. For enterprise-wide event, conduct formal post-incident review by deadline set by Incident Commander; assign corrective actions and due dates.

1. Readiness Requirements

Each business owner/service owner must maintain a current provider readiness record in the central repository designated and administered by ITSO. This applies to all third-party providers, prioritized first for critical and high-value providers under existing Virginia Tech risk-management criteria. ITSO establishes the implementation schedule and periodic review schedule.

- Business owner, service owner, provider name, and primary vendor contact.
- Critical/high-value designation; whether the service processes or accesses Virginia Tech data; and data classifications and data flows.
- Integrations, APIs, critical data flows, and technical owners for disablement and restoration.
- Administrative/service accounts, API keys, tokens, certificates, and other high-risk access methods.
- Applicable SLAs, incident-notification and escalation terms, contractual timeframes, emergency support channels, service-restoration provisions, and known provider cooperation/evidence-preservation obligations.
- Whether the service requires a Virginia Tech vanity URL, plus tested procedures for rapid DNS changes, certificate issuance, and redirection to an approved status or alternate page.
- Approved continuity or workaround procedures. Critical and high-value services must have an approved status page or alternate communication channel.

2. Assessment, Activation, and Leadership

- The service owner must notify ITSO immediately upon learning of a suspected provider outage or breach, even before provider confirmation, and promptly participate in the preliminary assessment.
- The CISO/Incident Commander determines whether the event is a cybersecurity incident, an operational outage, or both.
- For a cybersecurity event, the CISO/Incident Commander leads. For a non-security outage, the relevant IT service owner is Operational Incident Lead. For a mixed event, the CISO/Incident Commander leads overall response and the service owner leads operational recovery under that command.

- Activate the IMT only when the event has enterprise-wide or multi-unit impact, requires multiple departments and local/enterprise administrator support, or generates significant public or media attention.

3. Containment and Evidence

- ITSO/TRT directs technical assessment and containment. The service owner identifies affected business functions, data, integrations, credentials, and continuity impacts.
- When feasible and directed by ITSO/TRT, preserve Virginia Tech-side logs, configuration records, and other relevant evidence before changes are made.
- Request that the provider preserve relevant logs, evidence, and incident records to the extent permitted by the applicable contract and provider capabilities.
- Document all actions, including integration disablement, credential rotations, URL redirects, and restoration actions, in the incident record with action owner, timestamp, authorization, and outcome.
- When delay would increase harm, use emergency temporary authority described in Section 3 and promptly notify the VPIT-CIO and IMT, if activated.

4. Service Disablement, User Redirection, and Re-enablement

The CISO or Incident Commander may recommend the temporary disablement of a third-party service, implementation of user redirection measures, or subsequent service restoration. Authorization for these actions rests with the VPIT-CIO, in consultation with the service owner and the Incident Management Team (IMT) when activated.

Prior to approving service re-enablement, the service owner and the CISO/Incident Commander must validate that appropriate containment measures have been completed, required credential rotations have occurred (or documented exceptions have been approved), critical integrations have been reviewed, recovery activities are ready for execution, and any necessary assurances have been obtained from the service provider.

5. Post-Incident Review

Every enterprise-wide third-party outage or breach requires a formal post-incident review. The Incident Commander sets the due date based on severity and complexity. The review evaluates Virginia Tech’s readiness records, communications, decision-making, technical containment, recovery, and corrective actions; assigns owners and due dates; and identifies required updates to the provider inventory, readiness record, continuity procedures, and central repository.

Appendix I: AWS Account Compromise Playbook

This playbook applies to all AWS accounts, tenants, organizational units, and AWS-hosted services that process, store, transmit, or access Virginia Tech data. It supplements and follows the **Third-Party Outage and Breach Playbook**. Where AWS-specific procedures apply, this playbook provides additional direction.

Quick-Reference

Phase	Required Actions
First Hour	Notify ITSO immediately and create or update the incident record through 4HELP. Contact the AWS account/tenant manager. Identify the affected AWS account ID, organizational unit, services, business and service owners, potential data exposure, integrations, credentials, and operational impacts. Preserve available evidence and determine whether the event is a suspected compromise, an operational outage, or both.
Containment	ITSO/TRT directs AWS containment. Restrict or suspend affected access, services, integrations, or accounts as needed. Rotate or revoke relevant credentials in accordance with the Third-Party Outage and Breach Playbook unless the Incident Commander documents a written exception. Preserve logs, configurations, and other evidence before changes are made when feasible.
Communications	The Incident Commander sets the AWS, vendor, leadership, and stakeholder update cadence based on severity. Communications and Marketing coordinates external communications when needed. Legal Counsel and the CISO/Incident Commander approve communications before release.
Restoration	Validate required containment, credential rotation or documented exceptions, account ownership, configurations, integrations, and recovery actions before restoring service. The VPIT-CIO authorizes high-impact service re-enablement or user redirection in consultation with the service owner and IMT when activated.
Closure	Document all actions, approvals, communications, and outcomes in the incident record. For enterprise-wide incidents, complete a formal post-incident review by the deadline established by the Incident Commander and assign corrective-action owners and due dates.

1. Readiness Requirements

Each AWS account/tenant manager must maintain an AWS readiness record in the ITSO-designated central repository. This record must align with the requirements of the Third-Party Outage and Breach Playbook and include:

- AWS account ID;
- AWS organizational unit;
- AWS account/tenant manager;
- Business owner;
- Service owner;
- Critical/high-value designation using existing Virginia Tech risk-management criteria; and
- Current AWS support and escalation contacts.

Privileged-access details, including root credentials, IAM administrators, roles, access keys, federated access, break-glass access, and automation or service identities, must be maintained through existing AWS access-management records and made available to authorized incident responders when needed.

AWS account/tenant managers must maintain current procedures for:

- Contacting AWS Support and using applicable AWS escalation paths;
- Identifying the account owner and authorized technical contacts;
- Restricting or suspending access when directed;
- Identifying affected services, integrations, and business dependencies;
- Preserving available AWS logs, configurations, and evidence;

- Restoring services and validating normal operations; and
- Supporting continuity procedures for critical and high-value AWS-hosted services.

ITSO will establish the implementation and periodic-review schedule for AWS readiness records, consistent with the Third-Party Outage and Breach Playbook.

2. Assessment, Activation, and Leadership

Any person who identifies a suspected AWS account compromise, unauthorized activity, unexpected AWS resource consumption, credential exposure, or material AWS service disruption must immediately contact **4HELP** and notify ITSO.

The AWS account/tenant manager must promptly participate in the preliminary assessment and identify:

- The affected AWS account, organizational unit, region, service, application, or resource;
- Relevant business and service owners;
- Potentially affected data, integrations, users, credentials, and business functions;
- Potential operational, financial, legal, regulatory, or contractual impacts; and
- Available AWS support and escalation contacts.

The CISO/Incident Commander determines whether the event is a cybersecurity incident, an operational outage, or both.

For a cybersecurity incident, the CISO/Incident Commander leads the overall response. The CISO or DCISO may activate the TRT as needed. For an AWS operational outage without a suspected compromise, the relevant service owner leads operational recovery. For a mixed event involving an AWS outage and suspected or confirmed compromise, the CISO/Incident Commander leads the overall incident, with the service owner leading operational recovery under that command.

Activate the IMT only when the event:

- Involves multiple departments and requires local and enterprise administrator support;
- Has enterprise-wide or multi-unit impact; or
- Generates significant public or media attention.

3. Containment and Evidence Preservation

ITSO and the TRT direct technical assessment and containment for suspected or confirmed AWS compromise. The AWS account/tenant manager and service owner support those actions by identifying affected AWS resources, services, integrations, business functions, and continuity impacts.

When feasible and directed by ITSO/TRT, preserve relevant evidence before changes are made, including:

- CloudTrail and other available AWS logs;
- Security findings, alerts, and monitoring information;
- AWS configuration records, resource details, and account activity;
- Relevant billing, usage, and resource-consumption records;
- Identity and access-management records; and
- Virginia Tech-side logs, integration records, and configuration documentation.

Containment actions may include:

- Restricting or suspending affected access;
- Disabling or isolating affected AWS resources or services;

- Disabling affected integrations or data flows;
- Revoking sessions, keys, tokens, credentials, or other access mechanisms;
- Removing unauthorized identities, roles, policies, resources, or configurations;
- Restricting network access or public exposure; and
- Contacting AWS Support for assistance with containment, investigation, or restoration.

Following a suspected or confirmed compromise, rotate or revoke all relevant API keys, administrative credentials, service-account passwords, tokens, and certificates unless the Incident Commander documents a written exception in the incident record.

The AWS account/tenant manager may take immediate protective action only when an emergency requires immediate protection. Otherwise, ITSO or the CISO directs access restriction, account suspension, or other containment actions.

If the AWS account/tenant manager cannot be reached, placing an account in a suspended organizational unit requires CISO approval. When delay would materially increase harm, the CISO/Incident Commander may direct emergency suspension or other temporary AWS containment before standard approval, with the VPIT-CIO notified as soon as practicable and the action documented in the incident record.

Document all containment actions, including access restrictions, account suspension, credential rotation, service disablement, AWS communications, and restoration actions, in the incident record. Each entry must identify the action owner, timestamp, authorization, and outcome.

4. AWS Service Disablement, Suspension, and Re-enablement

The CISO/Incident Commander may recommend temporary disablement of an affected AWS-hosted service, suspension of an AWS account, restriction of access, or redirection of users to an approved status or alternate page when required to reduce risk.

For a high-impact AWS service, the VPIT-CIO authorizes service disablement, user redirection, and re-enablement in consultation with the service owner and IMT when activated.

Before seeking re-enablement authorization, the service owner and CISO/Incident Commander must validate, as applicable, that:

- The affected AWS account and services have been identified;
- Required containment actions have been completed;
- Relevant credential rotation or revocation has been completed, or a written exception has been documented;
- Unauthorized identities, configurations, resources, and access paths have been reviewed and remediated;
- Critical integrations and data flows have been reviewed;
- Required evidence has been preserved;
- AWS support information or assurances have been considered;
- Logging and monitoring are operating as expected;
- Required communications and notifications are complete or underway; and
- The service is ready for safe restoration.

5. Post-Incident Review

Every enterprise-wide AWS compromise or AWS outage requires a formal post-incident review. The Incident Commander sets the due date based on incident severity and complexity.

The review must evaluate Virginia Tech's:

- AWS readiness records and account ownership information;
- Detection, assessment, and escalation activities;
- Communications and decision-making;
- Technical containment and evidence preservation;
- Credential rotation, access management, and service recovery;
- Continuity and restoration procedures; and
- Corrective actions and long-term risk-reduction opportunities.

The review must assign corrective-action owners and due dates and identify required updates to the AWS readiness record, AWS account inventory, service continuity procedures, or the ITSO-designated central repository.

Appendix M: Acronyms

Acronym	Meaning
CISO	Chief Information Security Officer
DCISO	Deputy Chief Information Security Officer
IMT	Incident Management Team
ITSO	Information Technology Security Office
OARC	Office of Audit, Risk and Compliance
TRT	Technical Response Team
VPIT-CIO	Vice President for Information Technology and Chief Information Officer
SLA	Service Level Agreement
API	Application Programming Interface
PII	Personally Identifiable Information
FERPA	Family Educational Rights and Privacy Act
PCI	Payment Card Industry Data Security Standard

Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system, technology service, data, or related process.

Record of Changes

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
4.0	Randy Marchany	03/14/2014	`		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
5.5	Laura Gautier	3/7/2024			Various formatting changes, wording changes to Appendix F, added procedure on page 2
5.6	Randy Marchany	5/14/2024			Rearranged appendices, added IR Quick Start Guide
5.6-A	Randy Marchany	12/23/2024			Rewrote Sections 2 and 3; created new appendix for e-discovery
5.6-A	Randy Marchany	5/27/2025			Major structural changes made. Included Quick Step Guide
5.6-A	Randy Marchany	6/5/2025			Updated e-discovery and data recovery appendices
5.7	Randy Marchany	10/16/2025			Updating formatting
5.7-A Master	Randy Marchany	10/31/2025			Expanded Appendix E OmniSOC section
5.8 Master	Randy Marchany	12/17/2025			Added Cyber Incident Response RACI diagram
6.0	Robert Garbee	10/30/2026	David Raymond	10/30/2026	Major revisions to several sections to include 3rd party breach. Updated chart. Added 3rd party compromise

Earlier Record of Changes entries remain unchanged, including original names and dates.