

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.