REPORT IMMEDIATELY

Call 4HELP immediately at (540) 231-4357 (24x7) if you suspect an incident involves:

- High Risk data (this automatically applies to **all data in local or cloud systems/services**)
- Incidents with potential for severe financial, reputational, legal or regulatory impact
- Critical system disruption **due to security compromises**, including widespread incidents
- Unauthorized password, credential, account changes or **done with insider knowledge**

Remember: when in doubt, report it! CALL 911 IMMEDIATELY for any threats to life or property.

NON-URGENT REPORTING

REPORT A CYBERSECURITY INCIDENT HERE Report any network security event that might compromise:

- **Confidentiality** of moderate or low risk data
- **Integrity of:**
  - **Information** (including modification, deletion, and loss of access of moderate or low risk data)
  - **Devices** (malware infections, compromises, attacks and other similar incidents)
- **Availability of Virginia Tech resources** (including denial of service)

Information to provide to 4HELP or IT Security Office

- **Who** will be the security point of contact (name, email, phone #) for the unit?
- **What** symptoms do you observe?
- **Which** devices or accounts were affected, and what is their purpose? Please include IPs, host names, and domains. Identify devices or assets with high risk data.
- Is there a critical system disruption? Are the symptoms widespread?
- **What** risks do you believe may apply to this incident?
- **Who** was involved in this incident and what are their role(s) at Virginia Tech?
- Do you feel a person or system in your unit was targeted? If so, who or what was the target?
- **How** did you discover the incident?
- **When** did the incident occur?
- **What steps** have you taken since then? Please indicate who you've notified. (A timeline is helpful)
- **How** did the incident occur (if known)?

General Incident Guidelines

- **Stay calm.** Don't jump to conclusions, take aggressive action, or try to fix or investigate anything on your own. **Resist the urge to remediate before the full incident scope is known.**
- **Preserve evidence.** Don't allow systems to be modified or used. Don't change or investigate affected systems. If it's virtual system, make a clone. Copy logs to protect evidence.
- **Get guidance from ITSO and report any important updates.** ITSO will help you handle the incident through established, proven processes. The sooner ITSO knows of a change in scope, risk, or severity of the incident, the better we're able to protect the University.
- **Keep ITSO informed.** If you suspect your unit's email or phone systems have been compromised, **use a cell phone to provide updates to ITSO**.
- **Restrict information to those that need to know.** Share updates with leadership and those immediately involved with the incident, but **maintain as much confidentiality as possible**.
- **Document.** Write everything down while it's fresh: what was done, when it was done, and why it was done. Provide this information to ITSO.

WHEN to report

WHAT to report

WHAT to do next

Stage 1: Detection and Classification – IMMEDIATELY upon Incident Discovery

Your unit should:

- ❑ Let ITSO know if you discover an incident, or work with ITSO if we notify you that we've discovered an incident
- ❑ Gather information to provide to ITSO. **Make sure to include the information listed on the previous page.**
- ❑ Provide unit point of contact to ITSO

You can expect ITSO to:

- ❑ Discuss incident severity
- ❑ Begin gathering information

Stage 2: Containment and Preservation – WITHIN 15 minutes of Incident Discovery

Your unit should:

- ❑ Leave device(s) intact, but **do not** use or investigate on it/them
- ❑ If advised by ITSO, unplug network cable or disable network access from a firewall
- ❑ Preserve device state (for example, clone a virtual machine)
- ❑ Make a copy of log files
- ❑ **Document and communicate information on possible risks, including critical systems or data**
- ❑ Alert unit leadership of issue

Your unit should NOT:

- ❑ Shut down the device(s)
- ❑ Log on with elevated privileges to investigate
- ❑ Change the network settings on the device
- ❑ Issue/run commands or software
- ❑ Attempt to remotely scan the device
- ❑ **Attempt to fix anything or remove any problems before contacting the ITSO**

You can expect ITSO to:

- ❑ Coordinate plans for containment and investigation

Stage 3: Analysis, Eradication and Recovery – DAYS following Incident Discovery

Your unit should:

- ❑ **Prioritize incident above other workloads**
- ❑ Continue to gather and document information
- ❑ Perform a PII scan to look for notifiable data
- ❑ Work with ITSO to develop a recovery plan, including security enhancements
- ❑ Immediately report any new critical information to ITSO
- ❑ With ITSO guidance, restore affected services to operation
- ❑ Confirm system(s) are working properly following remediation

You can expect ITSO to:

- ❑ Coordinate incident handling
- ❑ Provide an incident analysis (timeline, scope, root cause and effects)
- ❑ Identify other at-risk systems, accounts or services
- ❑ Regularly share updates with unit and ITSO leadership
- ❑ Partner with unit to develop remediation plan
- ❑ Identify follow-up action items (notifications to affected individuals, offices, long-term security enhancements etc.)
- ❑ Continue to monitor for ongoing threats

Stage 4: Incident Closure and Follow-up – AFTER Incident is closed

Your unit should:

- ❑ Continue to work on long-term security enhancements
- ❑ Update internal documentation

You can expect ITSO to:

- ❑ Issue an executive incident closure report
- ❑ If necessary, coordinate with your unit to schedule post-incident "lessons learned" meetings
- ❑ Work with your unit to suggest security enhancements