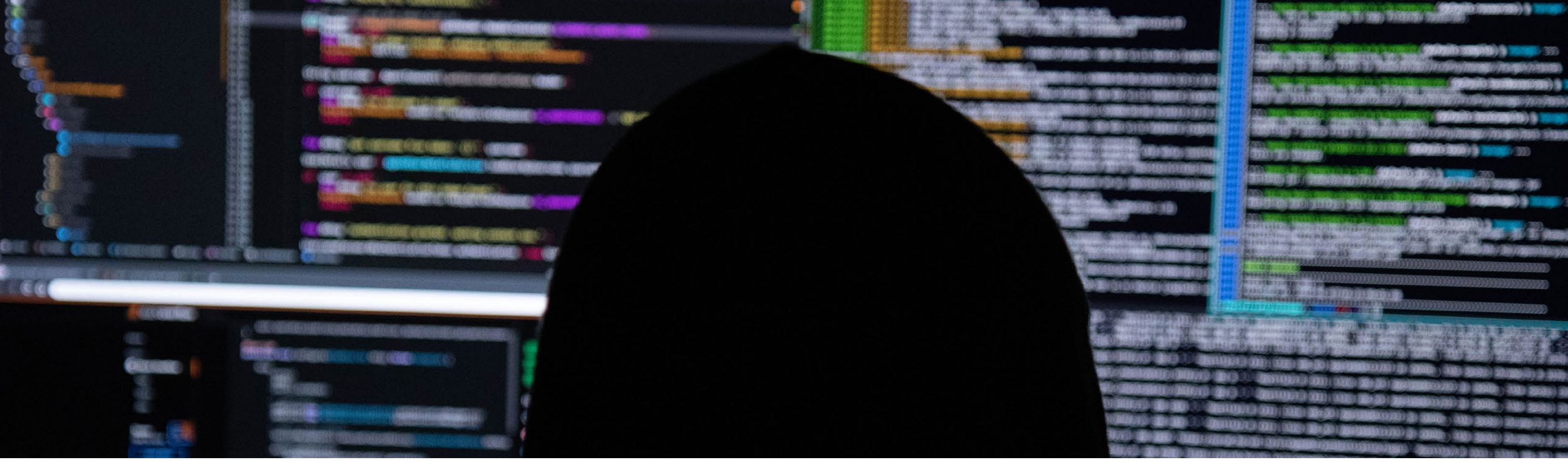
Cybersecurity Incident Planning for Institutes of Higher Education

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION



Preparing for a Cyber Attack

This Cybersecurity Incident Planning guide intends to provide direction and guidance to institutes of higher education seeking to improve their cybersecurity posture through cybersecurity risk management best practices. This guide is intended for any educational institution regardless of size. Schools can determine activities that are important to critical operation and customize practices recommended in this document accordingly. This guide recommends cybersecurity best practices and standards in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Identify and Protect

An important first step in improving a school's cybersecurity posture is to identify critical processes and assets. Ask yourself: what activities absolutely must continue in order to operate? Understanding what assets and resources support these critical functions, and the related cybersecurity risks, enables an educational institution to focus on and prioritize cybersecurity efforts.

Educational institutions should create and maintain a list of all hardware, software, and storage locations of sensitive data. It is important to inventory and monitor the networks, computers, and systems at your institution since these are entry points for cyber attacks. Schools should then identify and document threats, vulnerabilities, and risks to these critical assets.

Schools should also create and maintain cybersecurity policies that cover roles and responsibilities for employees and vendors with access to sensitive data. Cybersecurity policies should also include an incident response plan (IRP) in the event of a cyber attack.

Once critical infrastructure is identified, educational institutions should protect these critical assets by:

- Managing access to networks, computers, and sensitive information. Create unique accounts for each employee and use multi-factor authentication (MFA). Ensure users only have access to data, networks, and applications that are needed for their jobs.
- Encrypting sensitive data, both while stored on computers and when transmitted to other parties.
- Conducting regular backups of data and keeping an offline backup to protect against ransomware.
- Updating systems and software regularly, automating updates when possible.
- Having formal policies for safely disposing of electronic files and old devices. Securely delete and destroy data when no longer needed or required.
- Conducting regular cybersecurity trainings for employees. Ensure employees understand cybersecurity policies and their specific roles and responsibilities.

Report a breach to FSA by emailing CPSSAIG@ed.gov
or by filling out the Cybersecurity Breach Intake Form.

For more information on incident response preparation and creating an IRP, see NIST's Computer Security Incident Handling Guide.

Incident Response Plans

Before a cyber attack occurs, educational institutions should establish an IRP. Having well-established plans, procedures, and roles and responsibilities in place for responding to cyber attacks can help schools limit damage to their networks, expedite mitigation, and enhance law enforcement's ability to identify and apprehend perpetrators.

The IRP should be actionable and provide specific procedures to follow in the event of a cyber incident. The plan should also include timelines for critical tasks and identify key decision makers. Educational institutions should include the following in their IRPs:

- who has decision-making responsibility during a cyber incident, including implementing security and mitigation measures;
- how to contact critical personnel at any time and how to proceed if critical personnel are unreachable or unavailable;
- what mission-critical data, networks, assets, or services should receive priority during an incident;
- when and how to restore systems and backed-up data;
- measures for handling and preserving evidence;
- when and how to contact third parties who host affected data and services (e.g., cloud storage service providers or commercial data centers);
- contact information for the school's incident response firm or cybersecurity insurance company; and
- when and how to contact local federal law enforcement offices.

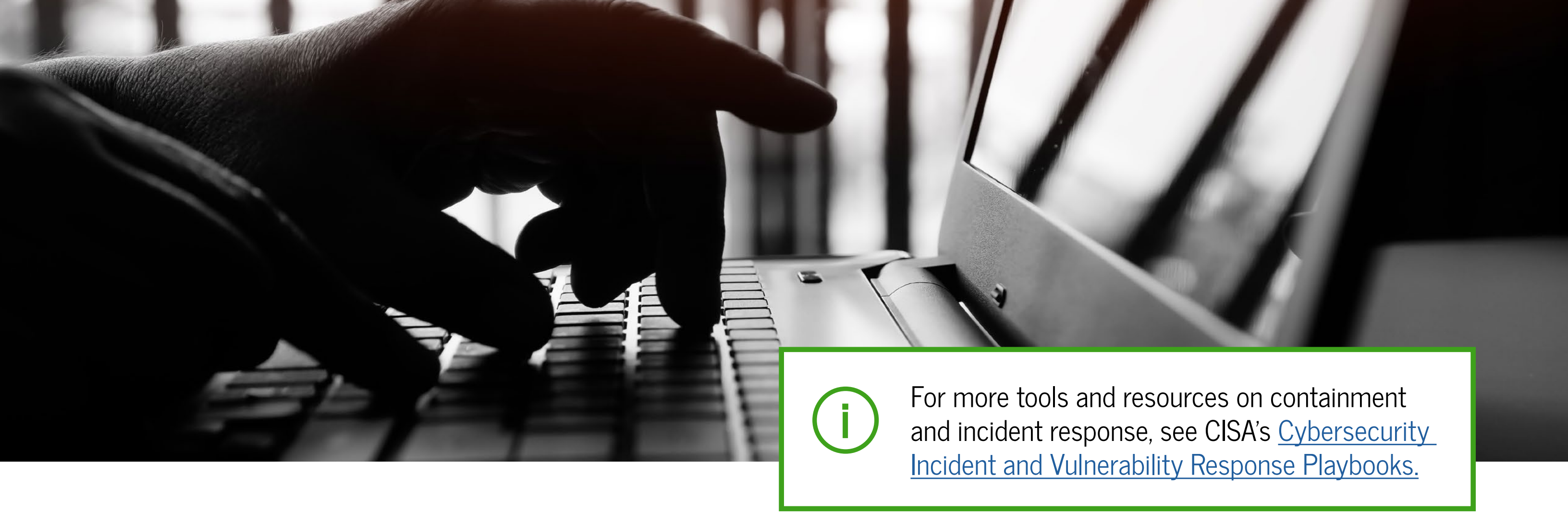
Attacks often affect online systems, email, telephone, and important files, so all personnel with incident response roles should have a printed copy.

Schools should also establish contacts with their local federal law enforcement agencies before a cyber incident occurs. Having a point-of-contact with law enforcement will help if an educational institution needs assistance during a cyber attack.

Test your plan.

Simulated exercises can help prepare staff for incident handling. If any gaps are identified during an exercise, update the IRP accordingly.

See NIST's Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities for more information on incident handling exercises.



For more tools and resources on containment and incident response, see CISA's Cybersecurity Incident and Vulnerability Response Playbooks.

Detect and Respond

Educational institutions should develop and test processes and procedures for detecting unauthorized access to networks, devices, and unauthorized personnel activity. Staff should be aware of their roles and responsibilities for detection and reporting.

If a school detects a cyber attack, first steps include activating the incident response plan and alerting internal leadership, legal counsel, and the communications team. Schools should immediately contact their cybersecurity insurance or incident response firm, if they have one, to determine next steps. Additionally, contact all vendors of affected systems.

The incident response team should rapidly perform an initial analysis to determine the incident's scope. The goal of this analysis is to examine data and discover all, or part of, an attack chain. Key events to document include:

- who or what originated the incident,
- what networks, systems, and applications are affected,
- how the incident is occurring (what tools or attack methods are being used and what vulnerabilities are being exploited),
- which users are logged onto the network,
- which systems and processes are running,
- current external connections to the computer systems, and
- all open ports and their associated services and applications.

Containment

Implementing a containment strategy is crucial before an incident overwhelms resources or increases damage to an educational institution. The objective of a containment strategy is to prevent further damage and to remove an intruder's access and control of systems. Quick decisions, such as shutting down systems or disconnecting servers, are critical and can be easier if procedures are outlined beforehand in a school's IRP.

Educational institutions should create separate containment strategies for major incident types, documenting options clearly for quick decision-making. When choosing a containment strategy, consider adverse impacts to a school's operations and services, duration, effectiveness (full vs. partial containment), and impact on evidence preservation.

Key containment activities include:

- isolate impacted systems and network segments;
- capture forensic images to preserve evidence;
- block (and log) unauthorized accesses and malware sources;
- close specific ports and mail servers, or other relevant servers and services; and
- reset system login credentials and revoke privileged access, if applicable.

Reporting

Educational institutions experiencing a cyber incident are encouraged to report it to their local federal law enforcement field offices. In addition, report the incident to the Cybersecurity and Infrastructure Security Agency (CISA), Federal Student Aid, and if there is a crime, the Federal Bureau of Investigation (FBI). For more information, including when and what to report, see the FBI's Cyber Incident Reporting guide.

Collect and Preserve Evidence

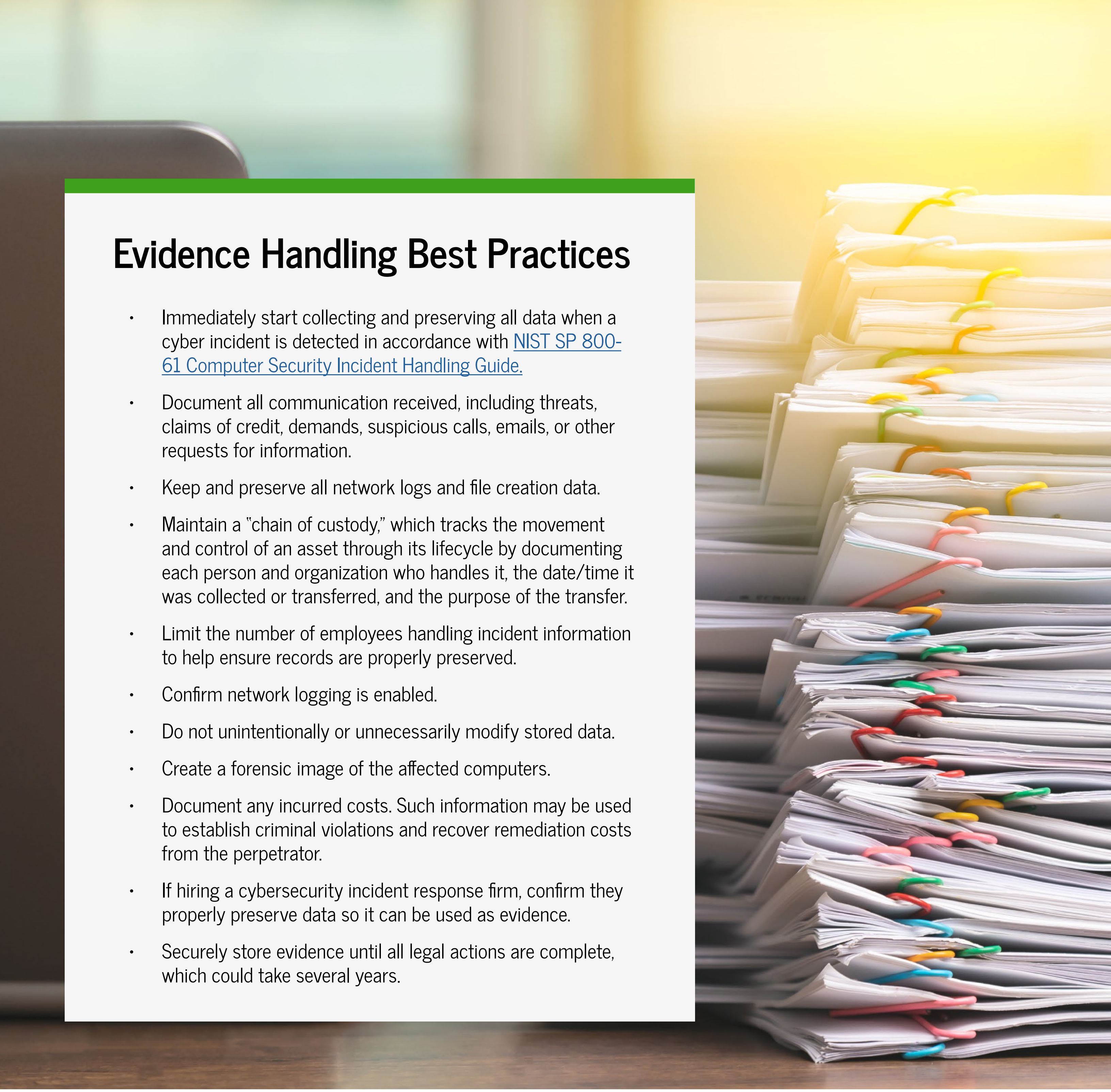
Every step taken from the time an incident is detected to its final resolution should be documented and timestamped. Detailed logs not only lead to efficient handling and resolution of an incident, but can also be used as evidence. Evidence logs should include:

- a description of all incident-related events, including dates and times;
- observed changes in files;
- systems, accounts, services, data, and networks affected by the incident and a description of how they were affected;
- the type and version of software being run on all affected systems;
- type of damage and cost inflicted by the incident, which can be important in criminal prosecutions; and
- name, title, and contact information of each person who collected or handled evidence.

Any communications received by the school, including demands, threats, or claims of credit, should be documented and preserved. Suspicious calls, emails, or other requests for information about the incident should also be documented.

A school's incident response team and system administrators should understand how to collect and preserve evidence during a cyber incident.

Report a breach to FSA by emailing CPSSAIG@ed.gov or by filling out the Cybersecurity Breach Intake Form.



Evidence Handling Best Practices

- Immediately start collecting and preserving all data when a cyber incident is detected in accordance with NIST SP 800-61 Computer Security Incident Handling Guide.
- Document all communication received, including threats, claims of credit, demands, suspicious calls, emails, or other requests for information.
- Keep and preserve all network logs and file creation data.
- Maintain a "chain of custody," which tracks the movement and control of an asset through its lifecycle by documenting each person and organization who handles it, the date/time it was collected or transferred, and the purpose of the transfer.
- Limit the number of employees handling incident information to help ensure records are properly preserved.
- Confirm network logging is enabled.
- Do not unintentionally or unnecessarily modify stored data.
- Create a forensic image of the affected computers.
- Document any incurred costs. Such information may be used to establish criminal violations and recover remediation costs from the perpetrator.
- If hiring a cybersecurity incident response firm, confirm they properly preserve data so it can be used as evidence.
- Securely store evidence until all legal actions are complete, which could take several years.

See NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response for additional information on proper forensic techniques.

Recovering After a Cyber Attack

Eradication

Schools should create eradication and recovery plans before a cyber incident occurs. After an incident is contained, activate eradication plans to eliminate components of the incident, such as deleting malware, disabling breached user accounts, and mitigating vulnerabilities that were exploited. Confirm there are no new signs of compromise and that vulnerabilities were patched to ensure threat actors cannot re-enter systems and networks. Educational institutions should coordinate with their incident response firm, cybersecurity insurance company, and law enforcement prior to initiating eradication efforts.

Key eradication activities include:

- remediate all infected IT environments (cloud, hybrid, host, and network systems);
- reimage affected systems;
- rebuild hardware;
- replace compromised files with clean versions;
- install patches;
- reset passwords on compromised accounts;
- monitor for any signs of adversary response to containment activities; and
- develop response scenarios for alternative attacks.

Schools should continue institution-wide monitoring after eradication efforts to monitor for any signs of adversary re-entry or use of new access methods.

ⓘ See NIST SP 800-61 Computer Security Incident Handling Guide for additional guidance on containment and eradication strategies.

Recover

A school's recovery plan should outline procedures to restore systems and networks to operation and confirm they are functioning normally after a cyber incident. Critical elements of a recovery plan include:

- formal recovery processes;
- list of the school's resources ranked in order of criticality (e.g., facilities, systems, external services);
- functional and security dependency maps to determine restoration priority;
- a list of personnel responsible for defining recovery criteria and implementing associated plans; and
- a comprehensive recovery communications plan with internal and external audience considerations.

Formal recovery processes should outline actions such as restoring systems from backups, rebuilding systems, replacing compromised files with clean versions, changing passwords, and tightening network security. Recovery planning should also include cost consideration for each recovery option.

See NIST SP 800-184 Guide for Cybersecurity Event Recovery for additional guidance, breach response scenarios, and recovery phase checklists.

Post-Incident Analysis

After concluding cyber incident recovery activities, educational institutions should conduct a post-incident analysis to review the effectiveness and efficiency of their incident handling and document lessons learned. The analysis should capture:

- incident root cause and mitigation efforts;
- infrastructure vulnerabilities and efforts to address;
- IRP problems or gaps;
- technical or operational training needs; and
- tools required to perform protection, detection, analysis, or response actions.

Educational institutions should update their IRP and update roles and responsibilities based on the post-incident analysis.

Contact Us

If you have any questions about the information included here, please email FSASchoolCyberSafety@ed.gov.

Visit our website:
fsapartners.ed.gov/title-iv-program-eligibility/cybersecurity

Resources

- Federal Student Aid Cybersecurity

  https://fsapartners.ed.gov/title-iv-program-eligibility/cybersecurity

- CISA Cybersecurity Incident and Vulnerability Response Playbooks

  https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

- CISA Insights: Chain of Custody and Critical Infrastructure Systems

  https://www.cisa.gov/sites/default/files/publications/cisa-insights_chain-of-custody-and-ci-systems_508.pdf

- Department of Justice Best Practices for Victim Response and Reporting of Cyber Incidents

  https://www.justice.gov/criminal-ccips/file/1096971/download

- NIST Cybersecurity Framework

  https://www.nist.gov/cyberframework/framework

- NIST Computer Security Incident Handling Guide

  https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

- NIST Guide for Cybersecurity Event Recovery

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

- NIST Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

  https://csrc.nist.gov/publications/detail/sp/800-84/final

- NIST Guide to Integrating Forensic Techniques into Incident Response

  https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf