State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	**No:** NYS-S13-005
IT Standard:	**Updated:** May 4, 2016
Cyber Incident Response	**Issued By:** NYS ITS **Standard Owner:** Enterprise Information Security Office

1.0 Purpose and Benefits of the Standard

This standard outlines the general steps for responding to computer security incidents. In addition to providing a standardized process flow, it (1) identifies the New York State (NYS) incident response (IR) stakeholders and establishes their roles and responsibilities; (2) describes incident triggering sources, incident types, and incident severity levels; and (3) includes requirements for annual testing, post-incident lessons-learned activities, and collection of IR metrics for use in gauging IR effectiveness.

The goals of IR, as outlined in this standard, are to:

- Confirm whether an incident occurred;
- Provide a defined incident notification process;
- Promote the accumulation and documentation of accurate information;
- Establish controls for proper retrieval and handling of evidence;
- Contain the incident and stop any unwanted activity quickly and efficiently;
- Minimize disruption to network operations;
- Provide accurate reports and useful recommendations to management; and
- Prevent and/or mitigate future incidents from occurring.

2.0 Enterprise IT Policy/Standard Statement

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the Office of Information Technology Services (ITS), the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-

engineering. Details regarding this authority can be found in NYS ITS Policy NYS-P08-002, Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines.

Except for terms defined in this standard, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

3.0 Scope

This standard applies to all State Entities (SE) responding to cyber security incidents involving SE information, and may serve as best practice for the State University of New York, the City University of New York, non-Executive branch agencies , NYS local governments and third parties acting on behalf of the State.

4.0 Information Statement

4.1 IR Stakeholder Roles and Responsibilities

In order to respond effectively to a computer security incident, it is critical that all IR stakeholders fully understand not only their roles and responsibilities in the IR process, but also the roles and responsibilities of each IR stakeholder. This is necessary to (1) avoid duplication of effort; (2) minimize procedural gaps that may occur; and (3) ensure rapid response to computer security incidents.

NYS IR stakeholders include:

1. State Chief Information Security Officer (CISO) – The State CISO, or his/her designee, provides for overall coordination of IR including the escalation of an incident. The State CISO leads the Enterprise Information Security Office (EISO) within the Office of Information Technology Services (ITS) which provides incident response services for NY State.

2. SE Leadership - Provides mainly IR oversight, with their Information Security Officer (ISO) or designee, being the most 'hands-on' in terms of IR management activities.

3. EISO Cyber Command Center – The Cyber Command Center serves as a central group for detection, analysis, tracking, response to and reporting of cyber threats and incidents. The Cyber Command Center responds to incidents by providing hands-on technical IR and will recommend steps for SE staff to remediate and mitigate such that it reduces the likelihood of future incidents.

   In addition, the Cyber Command Center facilitates collaboration and information sharing with other entities that may be experiencing the same or similar incidents, to help resolve the problem more quickly than if done separately. The Cyber Command Center collects statewide information on the types of vulnerabilities that are being exploited and the frequency of attacks and shares preventative information to help other SEs protect themselves from similar attacks.

4. First Responders - SE IT staff, such as network managers, system administrators, and other technical personnel, will be called upon, as needed, to provide support and tactical response to the Cyber Command Center. All digital forensic analysis must be performed by, or under the direction of, the Cyber Command Center.

5. Agency Incident Response Teams – SEs must have predefined teams at the ready which include, at minimum, Executive Management, Legal and the Public Information Officer. In some cases, Human Resources and Labor Relations may become involved.

6. External Entities - In consultation with the Cyber Command Center, external entities may conduct hands-on IR activities, such as investigative response activities, or may provide guidance. For example, a security solutions vendor may provide assistance on security appliance settings. External entities include vendors, service providers, or law enforcement including, but not limited to:
    - New York State Intelligence Center (NYSIC)
    - Multi-State Information Sharing and Analysis Center (MS-ISAC)
    - New York State Police
    - Federal Bureau of Investigation (FBI)
    - Internet Service Providers
    - Security Solutions Vendors
    - Data Holder Vendors

4.2 IR Process Flow

This IR process flow covers how to respond to specific situations for IR stakeholders to ensure an effective and efficient response. The focus of the NYS IR process is to eradicate the problem as quickly as possible, while gathering actionable intelligence, to restore business functions, improve detection and prevent reoccurrence. NYS has adopted a six step IR process flow as depicted below[1]:

Figure 4.1 - Incident Response Process Flow

[1]Based on the SANS Institute Incident Handling Step-by-Step

Step 1: Preparation

Proper planning and preparation for an incident before it occurs ensures a more effective and efficient IR process. Activities associated with this step, include establishing IR teams; updating IR tools, policies/procedures, and forms/checklists; and ensuring IR communication procedures and IR stakeholder contact lists are accurate and up-to-date. SEs must have a defined and up to date Contact List, and establish multiple communication channels with all entities and individuals on the IR Contact List.

SE's must assign responsibility for a central point of contact to coordinate identification and reporting up to the EISO. Typically this is performed by the SE's designated security representative. As per NYS Information Security Policy, all employees are required to report suspected information security incidents or weaknesses to the appropriate manager and designated security representative.

The Cyber Command Center will establish standard operating procedures (SOPs) for IR to reflect industry standards and best practice. These SOPs will be followed during incident response. Any exception must be documented. The Cyber Command Center must routinely vet and validate the tools and techniques used for IR. In order to operate efficiently and effectively, the IR process must be regularly tested. This must occur at least annually. This testing can be accomplished with mock incident training or tabletop exercises using realistic scenarios to provide a high-level outline and systematic walkthrough of the IR process and, to the extent possible, must include all IR stakeholders. These training scenarios must include specific 'discussion points' that represent key learning opportunities, and incorporate lessons-learned, which can then be integrated into the IR process as part of its review.

Step 2: Identification

Identification involves review of anomalies to determine whether or not an incident has occurred, and, if one has occurred, determining the nature of the incident. Identification begins with an event, an anomaly that has been reported or noticed in a system or network. Detection can be accomplished through technical sources (e.g., operations staff, anti-virus software), non-technical sources (e.g., user security awareness and reporting), or both.

It is important to recognize that not every network or system event will be a security incident. A first responder must be assigned to determine if there is an incident, categorize the incident and escalate as necessary. Typically, this will be the SE designated security representative.

To be effective in IR, incidents must be classified, and escalated as soon as possible to the proper IR stakeholders to promote collaboration and information sharing. Incident classification requires the use of established incident categories together with an incident severity matrix as a means for prioritizing incidents and determining appropriate IR activities.

<u>Incident Categories</u>

It is important to categorize common incidents experienced throughout the enterprise. By doing so, IR stakeholders can better focus their IR activities. It should be noted that incidents can have more than

one category and categorization may change as the investigation unfolds. NYS has adopted the six (6) US-CERT[2] incident categories as follows:

Incident Categories		
Category	Name	Description
0	Exercise / Network Defense Testing	Used during state, federal, international exercises and approved activity testing of internal/external network defenses or responses.
1	Unauthorized Access	An individual gains logical or physical access without permission to a NYS or local government network, system, application, data, or other resource.
2	Denial of Service	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 of or participating in the Denial of Service (DoS).
3	Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.
4	Improper Usage	A person who knowingly or unknowingly violates acceptable computing use policies.
5	Scans / Probes / Attempted Access	Includes any activity that seeks to access or identify a NYS or local government computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service. Unauthorized internal scans are considered incidents. Most external scans are considered to be routine, and on a case-by-case basis may require response and investigation.
6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Table 4.2 – Incident Categories

Incident Severity Matrix

All information security incidents should be categorized according to severity level to assist in determining the extent to which a formal IR is required. Severity levels are based on the perceived business impact of the incident. Severity levels may change as the investigation unfolds. General definitions and description of each severity level are as follows:

[2] http://www.us-cert.gov/government-users/reporting-requirements

Incident Severity Matrix		
Level	**Definition**	**Examples**
High	Incidents that have a severe impact on operations	Compromise of sensitive data Widespread malcode attack Unauthorized access to critical systems DoS affecting the entire enterprise
Medium	Incidents that have a significant impact, or the potential to have a severe impact, on operations	Small-scale DoS attack Website compromises Unauthorized access (brute force attacks against FTP, ssh, and other protocols)
Low	Incidents that have a minimal impact with the potential for significant or severe impact on operations	Network probes or system scans Isolated virus infections Acceptable use violations

Table 4.3 – Incident Severity Matrix

Escalation Procedures

During an incident, clear and effective communication is critical. As such, an escalation procedure should address all lines of communication in the event an incident occurs. This includes not only internal communication but external communications as well. Communication should flow through all involved IR stakeholders so that everyone has the necessary information to act and carry out their responsibilities in a timely manner. Notification must be made as soon as possible but should not delay an SE from taking appropriate actions to isolate and contain damage.

Each SE must have an IR escalation procedure that consists of (1) an escalation matrix, (2) an up-to-date contact list with alternate contacts, and (3) multiple communications channels, all in an effort to ensure appropriate and accurate information is disseminated quickly to the appropriate IR stakeholders.

Incident Scoping

Initial scoping is provided by the SE and includes:

- Identifying potential targets (e.g., known compromised systems, likely affected systems, key systems);
- Defining external touch points (e.g., Internet, wireless, 3rd party, remote access connections);
- Prioritizing likely scenarios (e.g., internal vs., external threat, targeted attack vs., target of opportunity); and
- Visualizing in-scope environment (e.g., network diagram, data flow).

Considerations for incident scoping activities are as follows:

- Relying on relevant and verified evidence sources;
- Reducing false positives and volume of data;

- Avoiding excessive scope and 'scope creep'; and
- Realizing operational and resource limitations may affect scope.

As additional incident-related information develops during the IR process and as additional stakeholders become involved, an incident typically requires re-scoping.

Incident Tracking & Reporting

A secure centralized tracking system, that can accommodate 'need to know' access, leads to a more efficient and systematic IR effort, as well as provides an audit trail should the efforts lead to legal prosecution of the threat.
At a minimum, documentation of the incident must contain the following information:

- Date / time the incident was reported
- Type of Incident
- Reporting source of incident
- Summary of the incident
- Current status of the incident
- All actions taken concerning the incident
- Contact information for all involved parties
- Evidence gathered during incident investigation
- Relevant comments from IR team members
- Proposed next steps to be taken

Step 3: Containment

This step focuses on containing the threat to minimize damage. It is during this step that information is collected to determine how the attack took place. All affected systems within the enterprise should be identified so that containment (and eradication and recovery) is effective and complete.

Incident containment involves 'stopping the bleeding' and preventing the incident from spreading. Containment can be accomplished by isolating infected systems, blocking suspicious network activity, and disabling services among other actions. Containment varies for each incident depending on the severity and risk of continuing operations. SE leadership makes decisions regarding containment measures based on recommendations from the EISO.

Step 4. Eradication

Eradication involves removing elements of the threat from the enterprise network. Specific eradication measures depend on the type of incident, number of systems involved, and the types of operating systems and applications involved. Typical eradication measures include reimaging infected systems and enhanced monitoring of system activity.

Analysis of information collected is an iterative process and occurs/reoccurs during both the containment and eradication phases.

Step 5. Recovery

Once the root cause of an incident has been eradicated, the recovery phase can begin. The goals of this step are to: (1) remediate any vulnerabilities contributing to the incident (and thus prevent future incidents) and (2) recover by restoring operations to normal. A phased approach is often used to return systems to normal operation, harden them to prevent similar future incidents and heighten monitoring for an appropriate period of time. Typical recovery activities include rebuilding systems from trusted images/gold standards, restoring systems from clean backups and replacing compromised files with clean versions.

Care must be taken to ensure that files restored from backup do not reintroduce malicious code or vulnerabilities from the incident and that the system is clean and secure before returning to production use. Once recovery has been completed, the IR lead must validate/certify that the incident has been resolved.

Step 6. Lessons Learned

An IR process is only as good as the ability to execute it successfully. Lessons learned can be the results of actual IR activities or IR capability testing, and these results should be used to improve the IR process by identifying systemic weaknesses and deficiencies and taking steps to improve on these. It is important that this take place relatively soon after the incident is closed.

Lessons learned, or post mortem, discussions provide (1) a record of steps taken to respond to an attack, (2) investigative results into determining the root cause of the attack, (3) potential improvements to make, such as IR stakeholder training and certifications, process and procedural updates, and technical modifications. Knowledge gained can be used in an effort to prevent and/or mitigate future incidents in the form of proactive services. This may include testing the IR process, conducting vulnerability assessments, providing computer security training, reviewing security policies and procedures, and disseminating cyber security reminders.

Both incident reports and the results of these lesson-learned discussions will be placed into a database for future use and shared with all IR stakeholders for situational awareness and professional development.

4.3 Incident Response Metrics

IR metrics must be compiled for each incident and reported to the EISO for enterprise situational awareness when possible and practical.

These metrics allow IR stakeholders (1) to measure IR effectiveness (and reveal potential gaps) over time; (2) identify trends in terms of threat activities and in doing so; (3) to provide justification for additional resources, to include additional personnel, training, and tools.

IR Metrics		
Category	Measurement	Description
Incidents	# Total Incidents / Year	Total amount of incidents responded to per year
	# Incidents by Type / Year	Total number of incidents by category responded to per year
Time	# Personnel Hours / Incident	Total amount of labor spent resolving incident
	# Days / Incident	Total amount of days spent resolving incident
	# System Down-Time Hours / Incident	Total hours of system down-time until incident resolved
Cost	Estimated Monetary Cost / Incident	Total estimated monetary cost per incident, to include containment, eradication, and recovery, as well as collection & analysis activities (this may include labor costs, external entity assistance, tool procurements, travel, etc.)
Damage	# Systems Affected / Incident	Total number of systems affected per incident
	# Records Compromised / Incident	Total number of records compromised per incident
Forensics	# Total Forensics Leveraged Incidents / Year	Total number of incidents requiring forensics (collection & analysis) per year
	# System Images Analyzed / Incident	Total number of system images analyzed per incident
	# System Memory Dumps Examined / Incident	Total number of system physical memory dumps examined per incident

Table 4.4 – Incident Response Metrics

5.0 Compliance

This standard shall take effect upon publication. The Policy Unit shall review the standard at least once every year to ensure relevancy. The Office may also assess agency compliance with this standard. To accomplish this assessment, ITS may issue, from time to time, requests for information to covered agencies, which will be used to develop any reporting requirements as may be requested by the NYS Chief Information Officer, the Executive Chamber or Legislative entities.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, SEs shall request an exception through the Enterprise Information Security Office exception process.

6.0 Definitions of Key Terms

Computer Security Event An anomaly that has been reported or noticed in a system or network.

Computer Security Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. A computer security incident is also defined as any event that adversely affects the confidentiality, integrity, or availability of system and its data.

Computer Network Defense (CND): Using defensive measures in order to protect information, information systems, and networks from threats.

Electronic Evidence: Electronic evidence as defined by the US DOJ Electronic Crime Scene Investigation is information and data of investigative value that is stored on or transmitted by an electronic device.

Incident Response: The manual and automated procedures used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events.

Incident Response Stakeholders: IR Stakeholders are any individuals – technical or non-technical, directly responding to or overseeing IR activities.

7.0 ITS Contact Information

Submit all inquiries and requests for future enhancements to the standard owner at:

Standard Owner
Attention: Enterprise Information Security Office
New York State Office of Information Technology Services
1220 Washington Avenue – Bldg. 7A, 4th Floor
Albany, NY 12242
Telephone: (518) 242-5200
Facsimile: (518) 322-4976

Questions may also be directed to the Enterprise Information Security Office at eiso@its.ny.gov

The State of New York Enterprise IT Policies may be found at the following website:
http://www.its.ny.gov/tables/technologypolicyindex.htm

8.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
11/15/2013	Original Standard Release; *replaces Office of Cyber Security Policy P03-001, Cyber Incident Reporting*	Thomas Smith, Chief Information Security Officer
11/21/2014	Standard Review – no changes	Deborah A. Snyder, Acting Chief Information Security Officer
03/20/2015	Clarified stakeholder roles/responsibilities, minor process changes	Deborah A. Snyder, Acting Chief Information Security Officer
05/04/2016	Changed Cyber Incident Response Team (CIRT) to Cyber Command Center	Deborah A. Snyder, Acting Chief Information Security Officer
11/21/2016	Scheduled Standard Review	

9.0 Related Documents

NIST SP 800-61, Computer Security Incident Handling Guide
NIST SP 800-83, Guide to Malware Incident Prevention and Handling
NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response
New York State Cyber Incident Reporting Procedures