# Table of Contents

1.0 Operational Standards Document Overview ................................................................. 3  
2.0 Establishment of CSIRT ................................................................................................. 3  
2.1 CSIRT Charge ............................................................................................................. 3  
2.2 CSIRT Overview ........................................................................................................ 3  
2.3 CSIRT Goals ............................................................................................................... 3  
2.4 CSIRT Objectives ...................................................................................................... 4  
3.0 CSIRT Organization .................................................................................................... 4  
3.1 Information Security Advisory Group (ISAG) ............................................................ 4  
3.2 CSIRT ...................................................................................................................... 4  
3.2.1 CSIRT – Chair ..................................................................................................... 4  
3.2.2 CSIRT - Core Team Members ............................................................................. 5  
3.2.3 CSIRT - Core Team Responsibilities ................................................................. 6  
3.2.4 CSIRT - Support Team Members ....................................................................... 6  
3.2.5 Support Team Responsibilities ............................................................................ 7  
3.2.6 CSIRT Relationship to Other Campus Departments ........................................... 8  
4.0 CSIRT Operational Resources .................................................................................... 8  
5.0 CSIRT Training .......................................................................................................... 9  
6.0 CSIRT Exercises ....................................................................................................... 9  
7.0 Incident Definition .................................................................................................... 9  
8.0 Reporting New Incidents & User Notification ............................................................. 9  
9.0 Incident Classification and Prioritization ................................................................. 10  
10.0 Incident Classification Escalation/De-escalation ...................................................... 11  
10.1 Incident Severity Escalation .................................................................................... 11  
10.2 Incident Severity De-escalation .............................................................................. 11  
11.0 Incident Investigation Process .................................................................................. 11  
11.1 Phase One - Identification and Assessment Steps .................................................... 12  
11.2 Phase Two - Containment and Eradication .............................................................. 12  
11.3 Phase Three - Recovery and Follow-up .................................................................. 12  
12.0 Incident Tracking ..................................................................................................... 13  
13.0 Incident Reporting .................................................................................................... 13  
14.0 Incident Closure ....................................................................................................... 13
1.0 Operational Standards Document Overview

This document defines the establishment of a computer security incident response team.

The Computer Security Incident Response Team (CSIRT) will follow the operational standards in this document. The standards provide a formalized approach to computer/network incident identification, investigation, and reporting.

The standards will be periodically updated to reflect the changing technology environment and campus needs. Request for changes to the CSIRT standards should be forwarded to the campus designated Information Security Manager (security@scranton.edu).

If there are conditions under which the applicability of the standards is unclear, it is the responsibility of the campus user to seek interpretive guidance from the Information Security Manager.

2.0 Establishment of CSIRT

2.1 CSIRT Charge

CSIRT is responsible for establishing, overseeing, and carrying out plans of action for any incident that potentially threatens the confidentiality, integrity, or availability of University electronic information assets and/or computing resources. The team will work closely with the Information Security Advisory Group (ISAG) on the development of operational procedures for and documentation of incidents.

Team members will develop policies and procedures for the prevention, identification, analysis, containment, and eradication of security threats. They will restore/recover the information or computing resource to an operational state as quickly as possible while preserving forensic data. Team members also serve as liaisons to the University department(s) where the incident occurs throughout the response process.

2.2 CSIRT Overview

The CSIRT is a group comprised of technology and functional specialists from the Planning and Information Resources (PIR) Division charged with the prevention, identification, analysis, containment, and eradication of computer/network security incidents. Security incidents are events that could adversely affect University of Scranton computer or network resources and/or cause loss of or damage to electronic information resources.

2.3 CSIRT Goals

The overall goal of the CSIRT is to protect and preserve electronic information and network assets to ensure the availability, integrity and, as required, confidentiality, of campus electronic information and network assets.
2.4 CSIRT Objectives

There are five primary objectives of CSIRT:

1. Control and manage the incident
2. Timely investigation and assessment of the severity of the incident
3. Timely recovery or bypass of the incident to normal operating conditions
4. Timely notification of serious incidents to senior campus administrators
5. The prevention of similar incidents in the future

3.0 CSIRT Organization

Campus response to computer/network security incidents is handled within a framework of the University of Scranton ISAG and CSIRT. The chair of CSIRT reports to the Associate Vice President of Planning and Information Management.

3.1 Information Security Advisory Group (ISAG)

The ISAG is charged with guiding the development and maintenance of University plans and policies designed to preserve the confidentiality, integrity, and availability of University electronic information assets and/or computing resources. The University of Scranton ISAG provides policy guidance and support for CSIRT.

3.2 CSIRT

CSIRT is the operational team of specialists responsible for conducting an incident investigation and recommending measures to correct or bypass a problem or condition relating to the incident. The nature of the incident will determine the actual role CSIRT will have in respect to implementing a corrective or preventive action.

The actual team consists of a core team who are assisted by support team members (subject matter experts), depending on the nature of a particular incident under investigation.

3.2.1 CSIRT – Chair

The Information Security Manager acts as CSIRT Chair. The chair approves initiation of a CSIRT investigation and CSIRT activities performed in support of the investigation. Responsibilities include:

- Convene CSIRT
- Conduct CSIRT meetings
- Coordinate CSIRT investigation
- Ensure incidents are classified according to severity class
- Determine investigation objectives
- Define/obtain resource requirements
- Communicate with external agencies
• Coordinate CSIRT training and exercises
• Prepare post-investigation "Lessons Learned" analysis
• Request support team resources
• Prepare CSIRT management reports
• Consult with PIR senior management on incidents classified with a moderate or high severity rating
• Communicate with senior department managers regarding incident investigation status
• Arrange for responsibility coverage during temporary absences

3.2.2 CSIRT - Core Team Members

CSIRT members include representatives from each information technology department within the PIR division.

These core team members are specialists with operating system, telecommunication, network, and/or database knowledge and skills. The Directors of Planning and Information Resources appoint the staff members to serve two year assignments on the CSIRT.

The Associate Vice President of Planning and Information Management will confirm the appointments.

Diagram of CSIRT Organization
3.2.3 CSIRT - Core Team Responsibilities

The primary responsibilities of the CSIRT are investigation and reporting. In order to carryout these responsibilities, the following support activities will be performed by the CSIRT:

- Maintain availability for 7x5 (M-F 08:30A-04:30p) communication access and incident response
- Develop and maintain incident classification scheme
- Monitor University of Scranton campus reporting mechanisms for reports of incidents
- Notify and consult with PIR senior management
- Assess scope of incident damage
- Classify incidents by severity
- Determine if incident can be investigated
- Control and contain incident
- Collect, document and preserve incident evidence
- Maintain chain of custody of all incident evidence
- Interview individuals involved in incident
- Conduct investigation to identify incident root cause or source, extent of damage, and recommended counter action
- Coordinate release of information with public relations staff
- Consult with law enforcement agencies, as authorized
- Follow all policies, laws, and regulations relating to privacy
- Prepare reports describing incident investigations
- Prepare recommendations to prevent future similar incidents
- Prepare recommendations to resolve incident and/or reduce impact of incident
- Prepare recommendations to bypass or correct conditions leading to incident
- Monitor recovery
- Identify CSIRT operational improvements
- Assist recovery from incident, where applicable

3.2.4 CSIRT - Support Team Members

Support members are not permanent CSIRT members. The support team members have expertise in particular subject matter that could be relevant to a CSIRT investigation. The CSIRT chair will determine when such expertise is required during an investigation. The support member will be added to the incident team at that time.

Any security incident investigation which includes a departmental computing system not under complete administrative control of PIR will be conducted by a minimum of two CSIRT members in addition to a representative of the department responsible for the computing system under review.

Support Team members will typically be drawn from the following areas:

- Departmental Technical Support Coordinator
When the target of the security incident is a departmental computing/network system, not administered by PIR staff, the CSIRT will include a Technical Support Coordinator from the impacted department. This CSIRT member will typically be a technical or administrative specialist who is responsible for supporting the system that is being misused or experiencing some other type of unauthorized activity. For example, if an incident involves a department email server, the CSIRT Chair will request the subject department to designate a technical or administrative CSIRT participant. This participant would be expected to possess the requisite experience and knowledge to assist in the investigation.

- Platform Specialists (e.g., Operating Systems, Applications, Hardware)
- Telecommunication Specialists (e.g., Network Infrastructure, Wireless, Telephones)
- Public Relation Specialists
- Human Resource Specialists
- Internal Auditors
- Public Safety/Law Enforcement Investigators

### 3.2.5 Support Team Responsibilities

The primary responsibilities of the CSIRT Support Team members are to assist CSIRT Core Team investigation and reporting. The Support Team members provide professional and technical expertise to the CSIRT core team in special subject knowledge areas. Typical responsibilities of Support Team members include:

- Assess scope of incident damage
- Assist classification of incidents by severity
- Assist determination whether incident can be investigated
- Assist control and containment of incident
- Collect, document and preserve incident evidence
- Maintain chain of custody of all incident evidence
- Interview individuals involved in incident
- Assist investigation to identify incident root cause or source, extent of damage, and recommended counter action
- Provide public communications guidance
- Provide guidance regarding law enforcement role
- Follow all policies, laws, and regulations relating to privacy
- Assist preparation of reports describing incident investigations
- Assist preparation of recommendations to prevent future similar incidents
- Assist preparation of recommendations to resolve incident and/or reduce impact of incident
- Assist preparation of recommendations to bypass or correct conditions leading to incident
- Assist in monitoring recovery
- Assist recovery from incident, where applicable
• Identify CSIRT operational improvements

3.2.6 CSIRT Relationship to Other Campus Departments

The following campus departments may also be involved with an incident:

• Computer Use Board
• Desktop and Instructional Resources
• Finance [Internal Auditor]
• Human Resources
• Network Resources
• Office of General Counsel
• Provost / Academic Affairs
• Public Relations
• Public Safety
• Residence Life
• Student Affairs [Judicial Affairs]
• Systems and Software Resources
• Technology Support Center

4.0 CSIRT Operational Resources

In order to conduct incident response investigations, CSIRT needs to acquire and maintain selected investigation tools. In addition, CSIRT needs to have a physically secure location to store investigation tools, conduct investigation analysis, and store material collected and/or prepared during the incident investigation. The following operational resources will be used by CSIRT:

• Hardware
  o Portable data storage devices
  o Workstations (Multi-OS or VMWare)
  o Forensic toolkit
  o Dedicated, Permanent High-Volume Storage Area

• Software
  o Forensic analysis
  o Forensic imaging
  o Password recovery
  o Encryption Software
  o Cryptographic Hash Utilities
  o Ticket / Incident Tracking System

• Miscellaneous Supplies
  o Photographic Imaging Equipment
  o Portable evidence storage containers
  o Spare backup media
  o Locking file cabinets
  o Secured physical room with restricted entry
5.0 CSIRT Training

CSIRT team members are required to obtain training and periodic updates in the following knowledge and skill areas:

- State and Federal Laws
- University of Scranton policies
- Investigative processes
- Evidence handling and protection
- Technical CSIRT hardware and software tools
- Testimony skills

6.0 CSIRT Exercises

The CSIRT will conduct an annual exercise that simulates a computer security incident. The purpose of the exercise will be to maintain the skills and knowledge of CSIRT members. The exercises will involve all CSIRT core team members. Support team members will be selected to participate as required by the nature of the exercise. At the termination of the drill, the CSIRT Chair will prepare a brief report to the ISAG evaluating the exercise. Any skill and/or knowledge area that needs to be improved as well as procedural enhancements will be identified in the report.

7.0 Incident Definition

For the purposes of this document, an incident is defined as an event that has actual or potential adverse effects on computer or network resources resulting in misuse or abuse, compromise of information, or loss or damage of property or information. Any such events that originate from, are directed towards, or transit University controlled computer or network resources will fall under the purview of CSIRT. This definition is purposely made inclusive, however it is foreseen that many events classified with a "limited" severity rating may be handled by semi-automated means and not require any further escalation.

Incident types include, but are not limited to: Compromised Machine, Denial of Service, Hoax, Malicious Code, Policy Violation, Probe, Unauthorized Access, Unauthorized Use.

8.0 Reporting New Incidents & User Notification

An incident can be reported through existing central reporting mechanisms at the Technology Support Center. A campus community member or anyone affected by a campus security incident should report a suspected incident by email (abuse@scranton.edu). In addition, CSIRT will coordinate with all PIR departments to ensure that CSIRT is notified of any reported problem that may reflect a security incident.

The individual reporting the incident will be asked to provide date, time, timezone, user contact information, brief description of the incident, and, if available, source and target network information.
Acknowledgement of a reported incident by CSIRT shall occur via an auto-generated response to email or web notifications. A telephone-reported incident will be acknowledged with a telephone call or email message from the CSIRT. All user reports will be analyzed, classified by severity rating, and an appropriate response will be generated. The scope of CSIRT response will be determined by the incident severity rating, or as directed by senior campus administrators.

If the nature of the incident cannot be reported via non-confidential methods, the incident may be directly reported to the Information Security Manager.

### 9.0 Incident Classification and Prioritization

Incidents will be analyzed and the severity of the incident classified according to several factors. As a guide, the overall severity classification of an incident will be higher based on the critical nature of the targeted system for the campus and broad negative organization and user impact of the incident. The overall severity classification of an incident will be reduced when there are readily available alternatives to remedy or bypass the problem situation. Severity ratings will be labeled as limited, moderate, or high.

The CSIRT will use the following table as a guideline in establishing incident severity.

<table>
<thead>
<tr>
<th>Incident Factors</th>
<th>Severity Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Limited</td>
</tr>
<tr>
<td>Criticality-Application</td>
<td>Non Tier 1 or 2 App</td>
</tr>
<tr>
<td>Criticality-Infrastructure</td>
<td>No</td>
</tr>
<tr>
<td>Impact-User/System</td>
<td>Affects a few people or a few systems</td>
</tr>
<tr>
<td>Impact-Public</td>
<td>None</td>
</tr>
<tr>
<td>Countermeasures</td>
<td>Solutions are readily available</td>
</tr>
<tr>
<td>Resolution procedures</td>
<td>Available and well-defined</td>
</tr>
</tbody>
</table>

Incidents receiving a "high" severity classification will receive the highest priority of CSIRT resources. In the case of multiple incidents, the higher severity rating incidents will receive higher priority CSIRT work assignment.

The incident severity classification will also determine the degree of involvement of campus senior managers in respect to the incident investigation. Moderate severity incidents may involve consultation with the Vice President for Planning and Chief Information Officer and/or the Associate Vice President of Planning and Information Management. High severity incidents will always involve consultation with the Vice President for Planning and Chief Information Officer and/or the Associate Vice President of Planning and Information Management.
10.0 Incident Classification Escalation/De-escalation

All new incidents will be assigned a severity rating by the CSIRT Chair in consultation with the CSIRT members. Such incident ratings may change over the course of an incident as more information about the incident becomes available and is reviewed by the CSIRT. The CSIRT Chair, in consultation with the CSIRT members, will determine if an incident rating should be escalated or de-escalated. The same criteria used to initially rate a newly reported incident will be used to escalate or deescalate an incident severity rating.

10.1 Incident Severity Escalation

If an incident is escalated to a "moderate" rating, the CSIRT Chair shall inform appropriate members of the University of Scranton management team via email about the incident and the reason for the escalation. This escalation shall be communicated to all CSIRT members.

If an incident is escalated from a "limited" or "moderate" severity rating to a "high" severity rating, the CSIRT Chair will review the incident with appropriate members of the University of Scranton management team via telephone or an ad hoc meeting. The University of Scranton management team members must approve the incident escalation. The Information Security Manager will notify the Vice President for Planning and Chief Information Officer and/or the Associate Vice President of Planning and Information Management in regards to any "high" severity rated incident and its possible campus impact.

10.2 Incident Severity De-escalation

The CSIRT Chair may determine an incident rating should be de-escalated to a "moderate" or "limited" category. If a "high" severity incident is downgraded to a "moderate" or "limited" severity rating, the CSIRT Chair must receive approval from appropriate members of the University of Scranton management team. In such cases, the reason for the de-escalation shall be documented within the incident investigation. The Vice President for Planning and Chief Information Officer and/or the Associate Vice President of Planning and Information Management shall be informed by the CSIRT Chair of the de-escalation and the reason for the action.

If the incident was previously rated as "moderate" and is downgraded to "limited", the appropriate members of the University of Scranton management team shall be informed about this action and the justification of the change. The other CSIRT members will be notified of the change.

11.0 Incident Investigation Process

The incident definition, defined in section 7.0, is purposely made inclusive, however it is foreseen that many events classified as “limited” may be handled by semi-automated means and not require any further escalation. Those events classified with a “limited” severity rating will follow standard procedures, customized to the units that perform those responsibilities. The incident investigation process defined in this section is geared toward incidents with a “moderate” or “severe” rating.
The incident investigation process follows the general objectives of investigation methodology, including:

- Conduct objective, thorough, and timely incident investigations
- Preserve individual privacy rights
- Collect, preserve, and protect incident/investigation data
- Maintain confidentiality as required
- Maintain thorough documentation of entire investigation process
- Safeguard investigation material/documentation
- Maintain chain of custody of investigation material/documentation
- Develop conclusions fully supported by facts in evidence
- Conduct a post-incident review of investigation, and document policy or procedural issues that enhanced or hindered the incident detection, monitoring, investigation, and subsequent development and implementation of corrective or problem bypass measures

11.1 Phase One - Identification and Assessment Steps

- Identify and verify problem (incident types and descriptions)
- Characterize the damage and extent of the problem, rate the incident severity
- Determine what investigation actions are to be taken
- Determine CSIRT resources are required to conduct the investigation, request/secure hardware, software, personnel resources
- Communicate with parties that need to be aware of the investigation

11.2 Phase Two - Containment and Eradication

- Collect and protect information associated with an incident investigation
- Contain the incident and determine further recovery or bypass actions to be taken
- Eliminate intruder's means of access and any related vulnerabilities

11.3 Phase Three - Recovery and Follow-up

- Return the systems to normal operations
- Close out the problem and follow up with a periodic post mortem review of the investigation. See "Incident Closure" section for details.
- Prepare and publish report, as required. If an incident has a rating of "severe", a brief formal report to PIR management shall be submitted upon closure of the incident. The report shall describe the incident, investigation methods, general conclusion, recommendations to avoid future related incidents and, if appropriate, lessons learned from the investigation.
12.0 Incident Tracking

The CSIRT will log, track and document the investigation and resolution of all security incidents. Where possible, software will be used to perform these functions. The CSIRT supporting software will generate a trouble ticket within the "security schema," a set of forms containing customized fields and actions.

The trouble ticket data for a particular incident investigation will only be available to the CSIRT members participating in the investigation. The trouble ticket data will not include any personally identifiable “confidential” information. Reports and summaries based on this data shall be generated as provided in Section 13, Incident Reporting.

13.0 Incident Reporting

The reports identified in this section will be generated from the incident tracking system. Where possible, these reports will be generated and distributed automatically:

Daily aging report: A daily report shall be sent via email to the CSIRT Chair on the status of the open tickets.

Monthly statistics report: A monthly report summarizing the incidents over the previous month shall be sent to University of Scranton PIR management.

Quarterly statistics report: A quarterly report shall be forwarded to PIR management containing a summary of incidents investigated during the previous quarter. The quarterly report will also include an evaluation of incident trends, including popular entry methods, prevention tips, and new tools.

Real-time Alerts: As determined appropriate by the Information Security Manager, alerts describing recent computer/network threats identified by CSIRT investigations and vulnerability prevention methods will be distributed on a timely basis. Such alerts may be distributed by web publications and/or other means, such as listservs.

14.0 Incident Closure

Once the systems have been returned to normal operations, the CSIRT will verify that all corrective and/or preventive tasks are complete and that local services have been restored. In cases where a division/department external to PIR is responsible for incident resolution, the CSIRT Chair will monitor and document incident resolution.

If an incident is rated as a “limited” severity, the CSIRT Chair or an individual designated by the CSIRT Chair may close it. If an incident is rated with a “moderate” severity, the CSIRT must approve closure of the incident. If an incident has received a “high” severity rating, University of Scranton management must approve closure of the incident.

At any time the CSIRT chair, the Associate Vice President of Planning and Information Management, and/or the Vice President for Planning and Chief Information Officer may terminate an incident investigation, regardless of
incident severity rating. If an incident is turned over to a law enforcement agency, the CSIRT incident investigation will, in most cases, be terminated.