

1. INTRODUCTION

When an information security situation is reported, the OIT evaluates its potential impact on the confidentiality, integrity or availability of University computer systems, networks or data. The OIT's security professionals may identify it as an *event* that requires further action. Following this evaluation and additional investigation, the Chief Information Officer may declare an event to be an information security *incident*, and make a preliminary determination of its potential severity. The severity level governs the level and type of response.

2. POLICY STATEMENT

This Policy specifies actions required of University personnel reporting or responding to an information security situation that may threaten the confidentiality, integrity or availability of University systems, networks or data.

- 2.1. All members of the University community are responsible for reporting known or suspected information security events promptly, as described in Section 6.1 of this document.
- 2.2. The University reserves the right to take necessary action under this policy to protect University resources or preserve evidence.
- 2.3. The Chief Information Officer (CIO) or designee is responsible for escalating a reported event as an incident, according to the criteria in Section 6.2 of this document, and for directing any action deemed necessary to facilitate incident response.
- 2.4. Individuals reporting or responding to an incident will follow the Information Security Incident Response Procedures and relevant sections of the Campus Emergency Preparedness and Response Plan.
- 2.5. All individuals involved in reporting or investigating an information security event or incident are obliged to maintain confidentiality, unless the CIO or cognizant University Officer authorizes information disclosure.
- 2.6. The CIO or designee must approve any exceptions to this policy or related procedures.

3. SCOPE

This policy applies to all individuals or entities using any University computer systems, networks or data.

4. TABLE OF CONTENTS

1. INTRODUCTION	1
2. POLICY STATEMENT	1
3. SCOPE	1
4. TABLE OF CONTENTS.....	2
5. DEFINITIONS.....	2
6. PROCEDURES.....	2
6.1. Reporting and Assessment.....	2
6.2. Classification.....	2
6.3. Response	3
6.4. Documentation.....	4
6.5. Evaluation and Testing	5
7. REFERENCE DOCUMENTS.....	5
8. CONTACTS	5

5. DEFINITIONS

Information Security Event	Any situation that <i>has the potential</i> to threaten the confidentiality, integrity or availability of University computer systems, networks or data. An event includes loss of control of University information through unauthorized access, equipment loss, or theft.
Information Security Incident	Any event that is <i>known or suspected</i> to have compromised the confidentiality, integrity or availability of University computer systems, networks or data. Only the CIO may declare that an event is an incident, following the procedures in Section 6.1 of this document.

6. PROCEDURES

6.1. Reporting and Assessment	Any member of the Notre Dame community who identifies an information security situation of potential concern should report it promptly through one of the following channels: <ol style="list-style-type: none">1. OIT Help Desk at (574) 631-8111 (business hours)2. OIT Operations Center at (574) 631-5603 (after business hours)3. Departmental or Distributed Support Services personnel4. Via e-mail to abuse@nd.edu
--------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Help Desk or OIT Operations personnel receiving a report will contact the appropriate first-level support for the system or application in question. If the reported event appears to meet one or more high severity criteria described in Section 6.2, the Help Desk or OIT Operations also will contact Information Security personnel to evaluate the event, and in cases of extreme severity or time-sensitivity, may also provide a preliminary notification to the CIO.

6.2. Classification	Upon consideration and assessment of an event notification, the CIO may declare a formal information security incident . An event
----------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------

will be considered an **incident** only if the CIO makes this declaration.

An information security **incident** falls into one of two categories:

A high severity incident is known or suspected to meet one or more of the following criteria:

1. Involves unauthorized access to, loss or theft of a device known to store, process or transmit highly sensitive information.
2. Involves an enterprise security device, such as a data center firewall, intrusion detection system, Tripwire system, or authentication service.
3. Involves compromise of an OIT-managed networking device, such as a router or switch.
4. Security monitoring devices (i.e., Tripwire, intrusion detection system) report an unauthorized change in the configuration of any device described in the first 3 points.
5. Causes the unavailability of a service critical to the University's mission.
6. Involves a significant number of University systems, indicating a widespread attack.
7. In the judgment of the CIO, poses a high severity risk to University systems or information.

A low severity incident is any information security incident that does not meet the foregoing high severity criteria.

The CIO determines the initial classification when declaring an incident, subject to later reclassification. A **high severity incident** is treated as a campus emergency, in accordance with the Campus Emergency Preparedness and Response Plan. All subsequent incident handling is governed by this plan.

6.3. Response

The highest priority is to protect the campus community and University resources. For all declared incidents, the priority of response will be:

1. protect human safety;
2. protect University resources;
3. contain damage or spread;
4. preserve evidence;
5. eradicate damage; and
6. restore systems and services.

If an incident meets one or more of the high severity criteria (as defined by the *Classification* procedure in Section 6.2), any member of the OIT Information Security Department may take and/or direct immediate action to protect University computer systems, networks or data. This includes, but is not limited to, the use of an attack-blocking facility, or the immediate and complete disconnection of a suspected compromised system from University networks. If this action is necessary, the Information Security staff

will notify the CIO or a Deputy CIO as soon as practical. OIT Information Security also may notify the administrator of the system, but such notification is *not* a **prerequisite** to actions necessary to protect University resources or preserve evidence. In cases when necessary to support an active investigation, or to preserve evidence, OIT Information Security may also take physical possession of any system believed to be involved in the event.

If, when responding to an incident, OIT Information Security discovers that credit cards have been compromised, we will follow published response requirements of the credit card brands in addition to Notre Dame's own response procedures.

Business Continuity During an Incident Investigation

Anyone who processes information should establish a business continuity/disaster recovery plan so that they can continue to conduct critical University business during an investigation. Business continuity will *not* take precedence over the activities required to contain damage or preserve evidence. Departments will handle outages that result from actions to contain the situation according to their pre-established business continuity/disaster recovery plans.

During the response to an incident, meetings and notifications will include the data steward(s) with responsibility for sensitive information involved. The CIO or designee will direct such actions as deemed necessary to respond. This authority includes, as appropriate, communication with other campus personnel.

The CIO is responsible for authorizing either the restoration of the system to operation or the continuing investigation.

6.4. Documentation

Upon formal declaration of an information security incident, OIT Information Security will prepare a summary of the relevant technical and operational details and provide it to the CIO.

If an incident extends beyond 24 hours, OIT Information Security will send the CIO updates, no less frequently than daily, on the status of the incident and remediation efforts.

Within four business days of the conclusion of an incident, OIT Information Security will prepare an incident report and provide it to the CIO.

The University will comply with all reporting requirements imposed upon it by law or contractual obligation. The Office of General Counsel will coordinate any such action.

6.5. Evaluation and Testing

OIT Information Security will coordinate an annual test of the incident response process.

The OIT Policy Administrator will coordinate an annual review of the Information Security Incident Response Policy and related procedures, following the Policy Review and Update Process.

7. REFERENCE DOCUMENTS

Policy or Document	Web Address
Campus Emergency Preparedness and Response Plan	http://emergency.nd.edu/
Highly Sensitive Information Handling Standards	http://oit.nd.edu/policies/itstandards/infohandling.shtml
Information Security Incident Response Procedures	See Section 6
Information Security Policy	http://oit.nd.edu/policies/itpolicies/infosec.shtml
Responsible Use of Information Technologies Policy	http://oit.nd.edu/policies/rup.shtml
Visa Cardholder Information Security Program – Actions if Compromised	http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html

8. CONTACTS

Subject	Office	Telephone Number	Email or URL
Policy Clarification	Office of the Chief Information Officer, OIT	(574) 631-9700	cio@nd.edu
Procedures	Information Security, OIT	(574) 631-5554	infosec@nd.edu
Web Address for this Policy	http://policy.nd.edu/policy_files/InformationSecurityIncidentResponsePolicy.pdf		