CORNELL UNIVERSITY
POLICY LIBRARY

Reporting Electronic Security Incidents

POLICY 5.4.2

Volume 5, Information Technologies
Chapter 4, Security
Responsible Executive: Chief Information Officer and Vice President for Information Technologies
Responsible Office: IT Security
Originally Issued: June 1, 2004
Full Review: December 13, 2017
Last Updated: December 13, 2017

POLICY STATEMENT

Users of information technology devices connected to the Cornell network must report all electronic security incidents promptly and to the appropriate party or office. The Information Technology Security Office has the responsibility to evaluate incidents for potential of a breach of institutional information, including personally identifiable information held by university, and, when necessary, initiate the Data Privacy Incident Response Team (DPIRT) process.

REASON FOR POLICY

The network constitutes a substantial university resource, and the university's missions rely significantly on a secure electronic communication network. Prompt and consistent reporting of electronic security incidents protects and preserves information technologies resources and institutional data and information, and aids the university's compliance with applicable law.

ENTITIES AFFECTED BY THIS POLICY

- All units of the university (Excluding the Weill Cornell Medical College)

WHO SHOULD READ THIS POLICY

- All members of the university community

WEB ADDRESS FOR THIS POLICY

- This policy: www.dfa.cornell.edu/treasurer/policyoffice/policies/volumes/informationtech/incidents.cfm
- University Policy Office: www.policy.cornell.edu

Cornell Policy Library
Volume 5, Information Technologies
Responsible Executive: CIO and Vice President for Information Technologies
Responsible Office: IT Security
Originally Issued: June 1, 2004
Last Updated: December 13, 2017

POLICY 5.4.2

Reporting Electronic Security Incidents

CONTENTS

Policy Statement 1
Reason for Policy 1
Entities Affected by this Policy 1
Who Should Read this Policy 1
Web Address for this Policy 1
Contents 2
Related Resources 3
Contacts 4
Definitions 5
Responsibilities 6
Principles 7
Procedures – Ithaca Campus Units 8
User 8
Local Support Provider 8
IT Security Office (ITSO) 9
Data Privacy Incident Response Team (DPIRT): Responsibilities and Processes 10
Responsibilities of the Chief Information Security Officer 10
Index 11

POLICY 5.4.2

Reporting Electronic Security Incidents

RELATED RESOURCES

University Policies and Documents
University Policy 4.6, Standards of Ethical Conduct
University Policy 4.12, Data Stewardship and Custodianship
University Policy 5.1, Responsible Use of Information Technology Resources
University Policy 5.4.1, Security of Information Technology Resources
University Policy 6.11.3 Employee Discipline (Excluding Academic and Bargaining Unit Staff)
Campus Code of Conduct
Code of Academic Integrity
Cornell University Policy Regarding the Abuse of Computers and Network Systems
Data Privacy Incident Response Team (DPIRT)
Ithaca Information Security and Privacy Advisory Committee (ISPAC)
Privacy of Electronic Communications at Cornell University
Procedures for Reporting Security Incidents

External Documentation
Financial Services Modernization Act
Health Insurance Portability Accountability Act (HIPAA)
Uniting and Strengthening American by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Acts (U.S.A Patriot Act)
U.S.C. Title 18, section 1030; Fraud and Abuse of Computers

POLICY 5.4.2

Reporting Electronic Security Incidents

CONTACTS

Direct any general questions about this policy to your college or unit administrative office. If any questions arise concerning specific issues regarding University Policy 5.4.2, Reporting Electronic Security Incidents, contact the following offices.

Contacts, Ithaca Campus Units

Subject	Contact	Telephone	E-mail/Web Address
Initial Contact for Questions	Local support provider	Device-specific	
Local Reporting			
Policy Clarification	IT Security Office	(607) 255-8421	security@cornell.edu www.it.cornell.edu/security/
Computers and Network Systems	Chief Information Officer and Vice President for Information Technologies	(607) 255-7445	www.cio.cornell.edu
Legal Issues	Office of University Counsel	(607) 255-5125	counsel.cornell.edu
Network Emergencies	IT Security Office	(607) 255-8421	security@cornell.edu www.it.cornell.edu/security/

POLICY 5.4.2

Reporting Electronic Security Incidents

DEFINITIONS

These definitions apply to terms as they are used in this policy.

Data Privacy Incident Response Team (DPIRT)	A committee that determines and guides the institution's response to the loss or exposure of university data. It is composed of representatives of University Counsel, Risk Management and Insurance, University Communications, Audit, IT Security, and the Cornell Police, and is chaired by the Chief Information Officer.
Electronic Security Incident	Electronic activities, such as “hacking” or a compromised or abused computer, that result in damage to or misuse of the Cornell network or a device connected to it.
Information Technology (IT) Device	Any device involved with the processing, storage, or forwarding of information making use of the Cornell information technology (IT) infrastructure or attached to the Cornell network. These devices include, but are not limited to, laptop computers, desktop computers, personal digital assistants, servers, and network devices such as routers or switches, and printers.
IP Address	*Internet Protocol Address.* A unique number associated with a device used for the routing of traffic across the Internet or another network.
IT Security Office (ITSO)	The office within Cornell Information Technologies (CIT) responsible for twenty-four hour monitoring, operational integrity, and security of the Cornell infrastructure, as well as responding to any events, including electronic security incidents, that affect the infrastructure.
Local Support Provider	An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an IT device (e.g., system administrator or network administrator). When there is no formally identified local support provider (e.g., a personally owned computer used from home to connect to the Cornell network) the user is the local support provider.
MAC Address	*Media Access Control Address.* A unique number assigned to the hardware within a device used for mapping its IP address.
User	An individual who uses an IT device.

RESPONSIBILITIES

The major responsibilities each party has in connection with this policy are as follows:

Chief Information Officer	When appropriate, decide on the institutional response to an information security incident.
Chief Information Security Officer	In response to direction from DPIRT, initiate breach reporting procedures. Maintain an archive of incident reports, submit quarterly incident metrics to DPIRT, and supply an annual summary of security incidents. Provide written reports of incidents for which the DPIRT process has been initiated.
Data Privacy Incident Response Team (DPIRT)	Determine and guide the university's response and actions after an information security incident. With input and guidance, define data types, the loss of which would warrant its consideration and notification. Periodically assess and approve data-loss analysis processes and incident response protocols used by the IT Security Office. Validate measures taken in response to a significant or widespread security incident.
Local Support Provider	Collect appropriate information regarding devices compromised by electronic security incidents. Disconnect affected information technology devices from the network, where appropriate. Notify security personnel of electronic security incidents and any remedial action taken.
Security Personnel	Open and maintain problem reports for electronic security incidents. Contact users of and/or local support providers for compromised devices. Communicate to local support providers and users, any actions that need to be taken, the reasons for them, the steps required to reestablish service, and any relevant technical information about the incident. Take appropriate actions to eliminate problem sources of traffic from the Cornell network, up to and including blocking the information technology device. Initiate escalation procedures, such as notification of the unit head, the Cornell Police, the Judicial Administrator, University Counsel, or University Audit, as necessary.
User	Report actual or suspected electronic security incidents to local support providers. In the event that the local support provider is unavailable, unwilling, or unable to correct an electronic security incident, disconnect the affected information technology device from the network by disconnecting the network connection. In the event that the local support provider is unavailable, unwilling, or unable to correct an electronic security incident, notify the Cornell IT Security Office (ITSO) at security@cornell.edu or (607) 255-6664.

POLICY 5.4.2

Reporting Electronic Security Incidents

PRINCIPLES

General Information

This policy fosters compliance with national privacy laws, protecting health care and financial information, state laws with respect to data breach notification, makes clear rules for custodians of electronic information to act in the event of a breach, and represents industry standard data security procedures.

POLICY 5.4.2

Reporting Electronic Security Incidents

PROCEDURES – ITHACA CAMPUS UNITS

User

If you suspect that an electronic security incident may have occurred or may be imminent, you are expected to take the actions detailed below.

◆**Note:** Symptoms that may indicate an electronic security incident include, but are not limited to, unusually sluggish computer performance; applications and/or windows opening without user prompt; generation of spontaneous emails; strange characters appearing in documents; system rebooting or shutting down for no apparent reason.

1. Contact the local support provider of the specific information technology (IT) device. Provide any necessary follow-up information.
2. In the event that the local support provider is unavailable, or unable to correct the electronic security incident, disconnect the affected IT device from the network by disconnecting the Ethernet plug in the back of the machine and notify the Cornell IT Security Office (ITSO) at security@cornell.edu or (607) 255-6664.

◆**Note:** In circumstances where the user is also the local support provider, the user is obligated to follow the procedures listed under Local Support Provider, below.

Local Support Provider

In the event of notification or identification of an electronic security incident, the local support provider must perform the following steps:

1. Contact the ITSO.
2. Disconnect the IT device from the network or take other actions that will otherwise limit damage to other IT resources. If not able to disconnect, contact the ITSO as in Step 3.
3. Collect all of the following relevant information. If you are unfamiliar with the terms below, or unable to collect this information, continue with Step 4.
   - The date and time of the incident, indicating time zone.
   - The IP and MAC address of the affected IT device, if known.
   - Other relevant IP and MAC addresses, if known (e.g., other IT devices affected, attacking source, etc.).
   - The function of the affected IT device (e.g., desktop computer, printer, scanner, production server, development server, file server, web server, workstation, lab device, etc.).

PROCEDURES, ITHACA CAMPUS UNITS, continued

- Distinguishing characteristics of the device (e.g., operating system, applications installed on the IT device, presence of antivirus software, firewalls, other security software, etc.).
- A description of the incident, including any relevant log entries, error messages, or other evidence indicating a problem with the IT device in question.
- The following information from the user of the device and/or information involved in the incident:
    - University role.
    - The legitimate business purpose for access to or use of the information.
    - Any other relevant information related to the incident.

4. Notify ITSO personnel at security@cornell.edu or (607) 255-6664. (Upon incident notification, security personnel will maintain a problem report and follow escalation procedures as necessary.)
5. Upon performing remedial actions, send e-mail notification to the ITSO at security@cornell.edu or call (607) 255-6664 for accurate closure of the problem report.
6. Notify affected user of remedial steps taken, recommended mitigating activities and other appropriate information.

IT Security Office (ITSO)

In the event of notification or identification of an electronic security incident, the ITSO will take the following actions:

1. Open a problem report.
2. Attempt to contact the user or local support provider for the compromised device.
3. Communicate to the user and/or local support provider of the device the actions that need to be taken, the reasons for them, the steps required to reestablish service, and any relevant technical information about the incident.
4. In the event that the user or the local support provider is unavailable, unable, or unwilling to correct the network security problem expeditiously, take whatever actions are necessary to eliminate the problem source of traffic from the Cornell network, up to and including blocking the IT device.
5. Under the guidance of the Chief Information Officer, if there is a reasonable suspicion of the loss or breach of institutional or university information, the

PROCEDURES, ITHACA CAMPUS UNITS, continued

ITSO will initiate the DPIRT process.

◆**Note:** The ITSO will initiate escalation procedures, such as notification of the unit head, the Cornell Police, the judicial administrator, university counsel, or University Audit, as necessary.

Data Privacy Incident Response Team (DPIRT): Responsibilities and Processes

DPIRT is convened whenever an information security incident occurs that puts institutional data or information at risk of loss or unauthorized disclosure. The primary purpose of this group is to determine and guide the university's response to an information security incident, up to and including the need to satisfy existing data breach notification statutes or processes as well as an institutional decision to notify individuals of a breach of their personally identifiable information.

The group will also:

- With the input and guidance of the data stewards, define data types the loss or unauthorized disclosure of which would warrant its consideration of notification.
- Periodically assess and approve the data-loss analysis processes and incident response protocols used by the ITSO.
- Validate measures taken in response to a significant or widespread security incident.

For more information on DPIRT, see Related Resources.

Responsibilities of the Chief Information Security Officer

The chief information security officer will provide a written report on the incident to the DPIRT prior to the breach notification process. Furthermore, he or she shall be responsible for writing up archived summary notes of the DPIRT meeting and decision. Finally, annually, the chief information security officer will provide a report to the DPIRT that includes a detailed overview of previous incidents, general mitigation approaches, and strategic initiatives for the purpose of preserving and protecting institutional data and information.

POLICY 5.4.2

Reporting Electronic Security Incidents

INDEX

Abuse of Computers and Network Systems 3
Access 5, 8
Administrator 5, 9
Cornell Police 5, 6, 9, 10
Custodian 7
Data Stewardship and Custodianship 3, 10, 11
Data Privacy Incident Response Team (DPIRT) 1, 5, 6, 10, 11
Director 4, 6, 10, 11
Disclosure 10, 11
E-mail 8
Emergencies 4
Financial Services Modernization Act 3
Forwarding 5
Health Insurance Portability and Accountability Act (HIPAA) 3
Intercepting 3
Judicial Administrator 6
Local Support Provider 4, 5, 6, 8, 9
Network security 9
Privacy 3, 7
Standards of Ethical Conduct 3
System administrator 5
Unit head 6, 9, 11
University Audit 6, 9, 10
University Counsel 4, 5, 6, 10