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

Last Full Review: July 23, 2019

Last Updated: July 23, 2019

POLICY STATEMENT

Users of Cornell's information technology resources must report all electronic security incidents immediately 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 for Ithaca-based locations and Cornell Tech; or the Security and Privacy Incident Response Team (SPIRT) for Weill Cornell Medicine campuses.

REASON FOR POLICY

Prompt and consistent reporting of electronic security incidents protects and preserves information technologies resources and institutional data and information, helps maintain required service levels and aids the university's compliance with applicable law.

ENTITIES AFFECTED BY THIS POLICY

☑ Ithaca-based locations

☑ Cornell Tech campus

☑ Weill Cornell Medicine campuses

WHO SHOULD READ THIS POLICY

– All members of the university community

WEB ADDRESS FOR THIS POLICY

– https://www.dfa.cornell.edu/policy/policies/reporting-electronic-security-incidents

CONTENTS

RELATED RESOURCES

University Policies and Documents Applicable to All Units of the University

University Policy 4.6, Standards of Ethical Conduct

University Policy 5.1, Responsible Use of Information Technology Resources

University Policy 5.5, Stewardship and Custodianship of Electronic Mail

University Policy 5.10 Information Security

Code of Academic Integrity

Cornell University Policy Regarding the Abuse of Computers and Network Systems

Ithaca Information Security and Privacy Advisory Committee (ISPAC)

University Policies and Documents Applicable to Only Ithaca-Based Locations and Cornell Tech

University Policy 4.12, Data Stewardship and Custodianship

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

Abuse of Computers and Network Systems

Data Privacy Incident Response Team (DPIRT)

Ithaca Information Security and Privacy Advisory Committee (ISPAC)

IT Security and Policy Resources

University Policies and Documents Applicable to Only Weill Cornell Medicine Campuses

Weill Cornell Medicine ITS policy 11.05 – Security and Privacy Incident Response Plan

External Documentation

Financial Services Modernization Act (a.k.a., The Gramm–Leach–Bliley Act)

General Data Protection Regulation (GDPR)

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

University Forms and Systems

Incident Response Questionnaire

CONTACTS – ITHACA-BASED LOCATIONS AND CORNELL TECH

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-Based Locations and Cornell Tech

Subject	Contact	Telephone	Email/Web Address
Initial Contact for Questions	Local support provider	Device-specific	
Local Reporting			
Policy Clarification	IT Security Office	(607) 255-8421	security-services@cornell.edu
Legal Issues	Office of University Counsel	(607) 255-5125	counsel.cornell.edu
Network Emergencies	IT Security Office	(607) 255-6664	security-services@cornell.edu
	IT Service Desk	(607) 255-5500	
Privacy Concerns	Privacy Officer	(607) 255-4096	privacy@cornell.edu
Cornell Hotline (Anonymous)		(866) 293-3077	hotline.cornell.edu

CONTACTS – WEILL CORNELL MEDICINE CAMPUSES

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.

Subject	Contact	Telephone	Email/Web Address
Incident Reporting	Your Supervisor (first contact)		
	ITS Support	(212) 746-4878	support@med.cornell.edu
Anonymous Reporting, or Reporting Directly to the Compliance Office	WCM Privacy Office	(646) 962-6930	privacy@med.cornell.edu
	WCM ITS Security	(646) 962-3010	its-security@med.cornell.edu
	Cornell Hotline (Anonymous)	(866) 293-3077	http://hotline.cornell.edu

DEFINITIONS

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

Cornell Information Technology Resources	All Cornell data, physical infrastructure, and devices (personally or university-owned) that store, process or interact with said resources. These devices include, but are not limited to, laptop computers, desktop computers, mobile devices, servers, and network devices such as routers or switches, and printers. Beyond devices, this can include third party services such as Infrastructure as a Service, Software as a Service or any other contracted service or solution.
Data Privacy Incident Response Team (DPIRT) Ithaca Based Locations and Cornell Tech	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, Privacy Officer, the Office of the University Controller, and the Cornell Police, and is chaired by the chief information officer.
Electronic Security Incident	An event that disrupts normal operations and may result in damage to or misuse of the university’s data or Cornell information technology resources. Examples of such events include attempts by unauthorized parties to access and/or disclose university data or make unauthorized changes, cases of password compromise, denial of service attacks, and malware.
IT Security Office (ITSO)	The office within Cornell Information Technologies (CIT) responsible for twenty-four hour incident response, monitoring, operational integrity, and security of the Cornell infrastructure, as well as responding to any events that affect the infrastructure, including electronic security incidents.
Local Support Provider	An individual, such as a desktop support technician or network administrator, with principal responsibility for the installation, configuration, security, and ongoing maintenance of an IT device. When there is no formally identified local support provider (e.g., a personally owned computer used from home to connect to IT resources) the user is the local support provider.
Security and Privacy Incident Response Team (SPIRT) Weill Cornell Medicine	A committee at Weill Cornell Medicine consisting of five core members: (1) Assistant Vice Provost of Information Services & Chief Information Officer, (2) Chief Information Security Officer, (3) Chief Privacy Officer & Senior Billing Compliance Officer, (4) Deputy University Counsel, and (5) Assistant Vice Provost of Communications & Marketing that determines and guides WCM’s response to the loss or exposure of university data.
Security Liaison	Designated local unit representative assigned to assist the IT Security Office throughout the incident.
User	An individual who interacts with Cornell information technology resources.

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	Lead security incident response efforts. Under the direction of the Data Privacy Incident Response Team (DPIRT), initiate breach-reporting procedures. Maintain an archive of incident reports, submit quarterly incident metrics to the DPIRT, and supply an annual summary of security incidents. Provide written reports of incidents to the CIO, DPIRT, and senior leadership, as appropriate.
Data Privacy Incident Response Team (DPIRT) Ithaca and Cornell Tech	Determine and recommend 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 (ITSO). Validate measures taken in response to a significant or widespread security incident.
IT Security Office (ITSO)	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 problems, up to and including blocking the information technology device. Initiate escalation procedures, such as notification to DPIRT, the unit head, and the security liaison when appropriate. Perform root cause analysis at incident resolution on significant or widespread security incidents.
IT Service Group Director	Receive reports from the security liaison regarding electronic security incidents. Author and maintain a local security incident response plan outlining appropriate escalation procedures.
Local Support Provider	Collect appropriate information regarding scope of compromise. Notify the ITSO of electronic security incidents and any remedial action taken.
Privacy Officer	In response to direction from DPIRT, initiate breach-reporting procedures for incidents including data subject to the General Data Protection Regulation (GDPR).
Security Liaison	Notify the ITSO of electronic security incidents and any remedial action taken. Assist the ITSO in identifying local unit personnel responsible for incident response collaboration. Facilitate status, remediation steps and incident conclusion reporting to responsible IT service group director.

RESPONSIBILITIES, continued

Security and Privacy Incident Response Team (SPIRT), Weill Cornell Medicine	Determine and guide the college’s response to an information security or privacy 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 or protected health information.
User	Report actual or suspected electronic security incidents to local support provider, including the sharing of notifications from vendors of suspected incidents.

PRINCIPLES

General Information

This policy fosters compliance with national and applicable international privacy laws and regulations, 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.

PROCEDURES

User

If you suspect that an electronic security incident may have occurred or may be imminent, whether through your own observation or a third-party notification, you are expected to take the actions detailed below.

Symptoms of an Electronic Security Incident

Symptoms that may indicate an electronic security incident include, but are not limited to, stolen or lost equipment; 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.

◆ **Note:** Lost or stolen personally owned devices that interact with Cornell information technology resources (including email), must be reported as an electronic security incident.

Reporting an Electronic Security Incident

If the user is also the local support provider, the user is obligated to follow the procedures listed below in the Local Support Provider section.

1. Immediately contact the local support provider upon identification of incident. Provide information needed to complete the Incident Response Questionnaire (see Related Resources).
2. In the event that the local support provider is unavailable (for example, if the incident occurs outside of normal business hours):
    - For all Ithaca-based locations and Cornell Tech campus, notify the Cornell IT Security Office (ITSO) at security-services@cornell.edu or (607) 255-6664
    - For Weill Cornell Medicine, notify WCM ITS Security at its-security@med.cornell.edu or (646) 962-3010.
    - Continue notification until confirmation is received from the ITSO or your local support provider.

Local Support Provider

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

1. Immediately notify IT Security Office :
    - For all Ithaca-based locations and Cornell Tech campus, notify the Cornell IT Security Office (ITSO) at security-services@cornell.edu or (607) 255-6664

PROCEDURES continued

- For Weill Cornell Medicine, notify WCM ITS Security at its-security@med.cornell.edu or (646) 962-3010.
- Continue notification until confirmation is received from the ITSO.

2. Ithaca-based campuses and Cornell Tech - complete the Incident Response Questionnaire (see Related Resources).
3. Weill Cornell Medicine – complete the WCM Incident Log Form. Please contact WCM ITS Security.
4. Collaborate with the IT Security Office throughout the incident until closure.

IT Security Office (ITSO), Ithaca and Cornell Tech

In the event of notification or identification of an electronic security incident, the ITSO will initiate the ITSO Incident Response Process by taking the following actions:

1. Attempt to contact the user or local support provider and security liaison.
2. Communicate to the user and/or local support provider the appropriate actions that need to be taken, the rationale, and path to remediation and recovery.
3. In the event that the user or the local support provider is unavailable, unable, or unwilling to correct the security problem expeditiously, take whatever actions are necessary to contain or remediate the incident.
4. Under the guidance of the chief information officer, the ITSO will initiate the Data Privacy Incident Response Team (DPIRT) process in the event of the loss or breach of university information.

WCM ITS Security, Weill Cornell Medicine

In the event of notification or identification of an electronic security incident, WCM ITS Security will initiate the Incident Response Process by taking the following actions:

1. Attempt to contact the user or local support provider.
2. Communicate to the user and/or local support provider the appropriate actions that need to be taken, the rationale, and path to remediation and recovery.
3. In the event that the user or the local support provider is unavailable, unable, or unwilling to correct the security problem expeditiously, take whatever actions are necessary to contain or remediate the incident.
4. Under the guidance of the assistant vice provost of information services and chief information officer, chief information security officer, or chief privacy officer, the core members of the Security and Privacy Incident Response Team (SPIRT) will be convened if the incident is deemed severe, and one that may result in the loss or breach of university information.

PROCEDURES continued

Security Liaison

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

1. Immediately notify IT Security Office personnel:
   - For all Ithaca-based locations and Cornell Tech campus, notify the Cornell IT Security Office (ITSO) at security-services@cornell.edu or (607) 255-6664
   - For Weill Cornell Medicine, notify WCM ITS Security at its-security@med.cornell.edu or (646) 962-3010.
   - Continue notification until verification is received.
2. Assist the support provider/and or user in completing the Incident Response Questionnaire (see Related Resources).
3. Collaborate with the IT Security Office throughout the incident until closure.
4. Facilitate status, remediation steps and incident conclusion reporting to responsible IT service group director.

Ithaca-Based Campuses and Cornell Tech: Data Privacy Incident Response Team (DPIRT)

The DPIRT is convened whenever an information security incident occurs that puts institutional data or information at risk of loss or unauthorized disclosure, or if an incident impacts institutional reputation. 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.

Additionally, the group is responsible for the following actions:

- 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.

PROCEDURES continued

Weill Cornell Medicine: Security and Privacy Incident Response Team (SPIRT)

The SPIRT is convened whenever an information security or privacy incident occurs that puts institutional data or information at risk of loss or unauthorized disclosure, or if an incident impacts reputational and/or financial harm to the institution or any affected individuals. 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 SPIRT team will follow the guidelines as set forth in the 11.05O – SPIRT Operations Manual for Weill Cornell Medicine.

Chief Information Security Officer

The chief information security officer will provide a written report on the incident to DPIRT or SPIRT (depending upon location of the incident), prior to the breach notification process. Furthermore, that individual is responsible to write up archived summary notes of the DPIRT or SPIRT meeting and decision. Finally, annually, the chief information security officer is required to provide a report to DPIRT or SPIRT 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.

INDEX