Drake Information Technology Services

REPORTING ELECTRONIC SECURITY INCIDENTS

POLICY STATEMENT

Users of information technology devices connected to the Drake network must report all electronic security incidents promptly and to the appropriate party or office as indicated in the Procedures section of this document.

REASON FOR POLICY

The network constitutes a substantial University resource, and the University's mission relies significantly on a secure electronic communication network. Prompt and consistent reporting of electronic security incidents protects and preserves this resource and aids in the University's compliance with applicable law.

ENTITIES AFFECTED BY THIS POLICY

- All units of the University.

WHO SHOULD READ THIS POLICY

- All members of the University.

WEBSITE ADDRESS FOR THIS POLICY

Drake University Policy Library: *drake.edu/policy*

Drake Information Technology Services

REPORTING ELECTRONIC SECURITY INCIDENTS

TABLE OF CONTENTS

POLICY STATEMENT 1
REASON FOR POLICY 1
ENTITIES AFFECTED BY THIS POLICY 1
WHO SHOULD READ THIS POLICY 1
WEB SITE ADDRESS FOR THIS POLICY 1
I. RELATED DOCUMENTS, FORMS, AND TOOLS 3
II. DEFINITIONS 3
III. RESPONSIBILITIES 3
IV. PURPOSE 4
V. PROCEDURES 5

1. USERS 5
2. LOCAL SUPPORT PROVIDER 5
3. NETWORK OPERATIONS CENTER (NOC) 7

Drake Information Technology Services

REPORTING ELECTRONIC SECURITY INCIDENTS

I. RELATED DOCUMENTS, FORMS, AND TOOLS

II. DEFINITIONS

Electronic Security Incident: Electronic activities—such as "hacking" or a compromised or abused computer—that result in damage to or misuse of the Drake network or a device connected to it.

Information Technology Device: Any device involved with the processing, storage, or forwarding of information that makes use of the Drake information technology infrastructure or is attached to the Drake network. These devices include, but are not limited to, laptop computers, desktop computers, servers, 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.

Local Support Provider: An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an information technology device (e.g., system administrator or network administrator).

MAC Address: Media Access Control Address. A unique number assigned to the hardware within a device used for mapping its IP address.

Network Operations Center (NOC): The functional service provided by ITS responsible for 24-hour monitoring, managing, and configuring of the Drake infrastructure, as well as responding to any events that affect the infrastructure, including electronic security incidents,

Subnet: A section of the University's distributed network.

User: Any individual who uses an information technology device such as a computer.

III. RESPONSIBILITIES

User

- Reports 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, disconnects the affected information technology device from the network by disconnecting the network connection.

Drake Information Technology Services

REPORTING ELECTRONIC SECURITY INCIDENTS

- In the event that the local support provider is unavailable, unwilling, or unable to correct an electronic security incident, notifies ITS personnel at informationsecurity@drake.edu or (515) 271-3001.

Local Support Provider

- Collects appropriate information regarding devices compromised by electronic security incidents.
- Disconnects affected information technology devices from the network, where appropriate.
- Notifies security personnel of electronic security incidents and any remedial action taken.

Drake Information Technology Services

- Opens and maintains problem reports for electronic security incidents.
- Contacts users of and/or local support providers of compromised devices.
- Communicates to local support providers and users, any actions that need to be taken, the reasons for them, the steps required to re-establish service, and any relevant technical information about the incident.
- Takes appropriate action(s) to eliminate problem sources of traffic from the Drake network, up to and including blocking the information technology device.
- Initiates escalation procedures, such as notification of the unit head, Drake Public Safety, University counsel, the provost, or the appropriate executive vice president.

IV. PURPOSE

To insure a viable, robust, and dependable network service and secure electronic communication network.

Drake Information Technology Services

REPORTING ELECTRONIC SECURITY INCIDENTS

V. PROCEDURES

1. USERS

NOTICE

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, or the system reboots or shuts down for no apparent reason.

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

1. Contact any of the following members of the Drake Information Technology Services leadership team:
    a. The Chief Information Technology Officer
    b. An ITS director

2. Inform the local support provider of the specific information technology device. Provide any necessary follow-up information.

3. In the event that the local support provider is unavailable, or unable to correct the electronic security incident, disconnect the affected information technology device from the network by disconnecting the Ethernet plug in the back of the machine and notify ITS personnel at informationsecurity@drake.edu or (515) 271-3001.

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.

2. 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) Notify ITS personnel at informationsecurity@drake.edu or (515) 271-3001. (Upon incident notification, ITS staff will create and maintain a problem ticket and follow escalation procedures as necessary.)

Drake Information Technology Services

REPORTING ELECTRONIC SECURITY INCIDENTS

2) Disconnect the information technology device from the network or take other actions that will otherwise limit damage to other IT resources.

3) Collect all of the following relevant information. If you are unfamiliar with the terms below, or unable to collect this information, contact Drake Information Technology Services.
   - Date and time of the incident, indicating time zone.
   - IP and MAC address of the effected information technology device, if known.
   - Other relevant IP and MAC addresses, if known (e.g., other information technology devices affected, attacking source, etc.)
   - Function of effected information technology device (e.g., desktop computer, printer, scanner, production server, development server, file server, web server, workstation, lab device, etc.)
   - Distinguishing characteristics of the device (e.g., operating system, applications installed on the information technology device, presence of anti-virus software, firewalls, other security software, etc.)
   - Description of the incident, including any relevant log entries, error messages, or other evidence indicating a problem with the information technology device in question.

4) Upon performing remedial actions, send mail notification to ITS staff at informationsecurity@drake.edu or call (515) 271-3001 for accurate closure of the problem report.

5) Notify effected user of remedial steps taken, recommended mitigating activities, and other appropriate information.

3. NETWORK OPERATIONS CENTER (NOC)

NOTICE

The NOC will initiate escalation procedures, such as notification of the unit head, Drake Public Safety, University counsel, the provost, or the appropriate vice president.

In the event of notification or identification of an electronic security incident, the ITS Network Operations Center (NOC) 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) Inform 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 re-establish service, and any relevant technical information about the incident.

4) Take appropriate action to preserve compromised data or user account access logs for evidentiary purposes.

5) In the event that the user or 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 Drake network, up to and including blocking the information technology device.