Incident Response Policy
USG Policy 6 (1.20) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

This policy is intended to ensure that USG is prepared if a security incident were to occur. It details exactly what must occur if an incident is suspected, covering only electronic, but not exclusively physical security incidents. Note that this policy is not intended to provide a substitute for legal advice, and approaches the topic from a security practices perspective.

The scope of this policy covers all information assets owned or provided by USG, whether they reside on the corporate network or elsewhere. This policy will be reviewed annually to ensure continual compliance with USM IT Security Standards and other pertinent policies, laws and industry standards.

The Universities at Shady Grove is hereinafter referred to as "USG" and the Office of Information Technology as “OIT.” This policy will be reviewed annually to ensure continual compliance with USM IT Security Standards and other pertinent policies, laws and industry standards.

II. Definitions

A. *Confidentiality***:** a set of rules or procedures that limits access or places restrictions on certain types of information.

B. *Encryption*: the process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

C. *Malware*: short for "malicious software." A software application designed with malicious intent. Viruses and Trojans are common examples of malware.

D. *Mobile Device*: a portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

E. *PDA*: stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

F. *Smartphone*: a mobile telephone that offers additional applications, such as PDA functions and email.

G. *Trojan*: also called a "Trojan Horse." An application that is disguised as something innocuous or legitimate, but harbors a malicious payload. Trojans can be used to

covertly and remotely gain access to a computer, log keystrokes, or perform other malicious or destructive acts**.**

H. *Virus*: also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

I. *WEP*: stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

J. *WPA*: stands for WiFi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

III. Types of Incidents

A. For the purposes of this policy a security incident is defined as one of the following:

1. Electronic: This type of incident can range from an attacker or user accessing the network or system for unauthorized/malicious purposes. This includes, but not limited to malware infections, theft of electronic data, unauthorized system/data alterations, etc.

2. Physical: A physical IT security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain USG information.

B. All incidents must be reported in a timely fashion to OIT.

IV. Preparation

A. Work done prior to a security incident is arguably more important than work done after an incident is discovered. The most important preparation work is maintaining good security controls that will prevent or limit damage in the event of an incident. This includes technical tools such as firewalls, intrusion detection systems, authentication, and encryption; and non-technical tools such as good physical security for laptops and mobile devices. Additionally, prior to an incident, USG must ensure that the following is clear to OIT personnel:

1. What actions to take when an incident is suspected

2. Who is responsible for responding to an incident

B. USG should review any industry or governmental regulations that dictate how it must respond to a security incident (specifically, loss of USG data), and ensure that its incident response plans adhere to these regulations.

V. Confidentiality

A. All information related to an electronic or physical security incident must be treated as confidential information until the incident is fully contained. This will serve both to

protect individual reputations (if an incident is due to an error, negligence, or carelessness) and to control the release of information to the media and/or USG community.

VI. Notification

A. All electronic and physical incidents involving the compromise of personal information (as defined under State Government Article 10-301, Section III) must be reported to the USM Office of the Chief Information Officer. Notices of OIT incidents and advisories to the institutional user community will be carried out by the Director of OIT or designee.

VII. Managing Risk

A. Managing risk of a security incident or data loss is the primary reason to create and maintain a comprehensive security policy. Risks can come in many forms: electronic risks like data corruption, computer viruses, hackers, or malicious users; or physical risks such as loss/theft of a device, hardware failure, fire, or a natural disaster. Protecting critical data and systems from these risks is of paramount importance to USG.

B. Risk Assessment

1. As part of the risk management process, USG must conduct an accurate and thorough assessment of the potential risks (man-made and natural) and any vulnerabilities to the confidentiality, integrity, and availability of USG's critical or confidential information. An assessment must be thorough, can be performed by USG personnel or external consultants (or both), and must be well documented.

C. Risk Management Program

1. A formal risk management program must be implemented to cover any risks known to USG (which should be identified through a risk assessment), and ensure that reasonable security measures are in place to mitigate any identified risks to a level that will ensure the continued security of USG's confidential and critical data.

VIII. Enforcement

A. The enforcement of this policy will be carried out by authorized USG OIT personnel designated by the Director of OIT and USG Senior Leadership. Violations may result in disciplinary actions, which may include suspension, restriction, or revocation of access. Where illegal activities or theft of USG property (physical or intellectual) are suspected, USG may report such activities to the state/federal law enforcement authorities.

IX. Revision History

Date	Description	Revised By
11/28/2018	Initial Policy Creation	Russell Schlosburg

X. Related Documents

A. USM IT Security Standards v4
http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf