

Section 1	<b>IT Security Policies</b>	12/08/14	-Effective
Incident Management		06/05/18	-Revised
		John Wells	-Author

**Introduction**

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some the actions that can be taken to reduce the risk and drive down the cost of security incidents.

**Purpose**

This document describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of Information Resources as outlined in the Email Policy, the Internet Policy, and the Acceptable Use Policy.

**Audience**

The CCM Incident Management Policy applies equally to all individuals that use any CCM Information Resources.

**Definitions**

**Information Resources (IR):** Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

**IT Director / Network Administrator:** Responsible for CCM IT information resources. The designation of the IT Director/Network Administrator is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the company’s information activities, and ensure greater visibility of such activities within all parts of the company. The IT Director has been given the authority and the CCM Ownership Group to implement Security Policies, Procedures, Practice Standards and Guidelines to protect the Information Resources of the company.

Section 1	<b>IT Security Policies</b>	12/08/14	-Effective
Incident Management		06/05/18	-Revised
		John Wells	-Author

**Definitions, continued**

**Computer Incident Response Team (CIRT):** Personnel responsible for coordinating the response to computer security incidents in an organization

**Virus:** A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allow users to generate macros.

**Worm:** A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network using otherwise unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners, and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

**Trojan Horse:** Destructive programs—usually viruses or worms—that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or on a diskette, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board.

**Security Incident:** In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

**Vendor:** someone who exchanges goods or services for money.

Section 1	<b>IT Security Policies</b>	12/08/14	-Effective
Incident Management		06/05/18	-Revised
		John Wells	-Author

**Incident Management Practice Standard**

- CCM CIRT members have pre-defined roles and responsibilities which can take priority over normal duties.
- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
- The IT Director is responsible for notifying the CIRT and initiating the appropriate incident management action.
- The IT Director is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- The appropriate technical resources from the CIRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- The IT Director will determine if a companywide or subset communication is required, the content of the communication, and how best to distribute the communication.
- The appropriate technical resources from the CIRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
- The IT Director is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIRT.
- The CCM IT Director is responsible for reporting the incident to the:
  - ❖ Internal company personnel
  - ❖ External parties affected by said incident, i.e. customer base.
  - ❖ External support groups, i.e. third party IT support, software development group.
  - ❖ Local, state or federal law officials as required by applicable statutes and/or regulations
- The IT Director is responsible for coordinating communications with outside organizations and law enforcement.
- In the case where law enforcement is not involved, the IT Director will recommend disciplinary actions, if appropriate, to the CCM Ownership Group.
- In the case where law enforcement is involved, the IT Director will act as the liaison between law enforcement and CCM.

**Disciplinary Actions**

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and

Section 1	<b>IT Security Policies</b>	12/08/14	-Effective
Incident Management		06/05/18	-Revised
		John Wells	-Author

volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of CCM Information Resources access privileges, civil, and criminal prosecution.

**Supporting Information** **This Security Policy is supported by the following Security Policy Standards.**

**Reference #** **Policy Principle detail**

- 3 All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
- 6 The use of IR must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Personnel responsible for the custody and operation of computers shall be responsible for proper authorization of IR utilization, the establishment of effective use, and reporting of performance to management.
- 7 Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.
- 16 Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.

**Supporting Information, continued** **This Security Policy is supported by the following Security Policy Standards.**

**Reference #** **Policy Standard detail**

- 21 All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The CCM IT Director reserves the right to remove any unlicensed software from any computer system.
- 22 The CCM IT Director reserves the right to remove any non-business related

Section 1	<b>IT Security Policies</b>	12/08/14	-Effective
Incident Management		06/05/18	-Revised
		John Wells	-Author

---

software or files from any system. Examples of non-business related software or files include, but are not limited to; games, instant messengers, pop email, music files, image files, freeware, and shareware.