

PALM BEACH STATE COLLEGE

ADMINISTRATIVE PROCEDURE

Policy: 6Hx-18-1.XX	Category: Information Technology	Version Date: 0001
Title: Information Security Incident Management		Effective Date: 11-01-09
Originating Unit: Information Technology Security Office		Last Review: TBD
Review Officer: Chief Information Officer, Anthony Parziale		Next Review: TBD

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 Information Security and Acceptable Use policies.

Scope:

The Palm Beach State College Information Security Incident Management Procedures applies equally to all individuals that use any Palm Beach State Information Resources.

Definitions:

Information Technology Security Office (ITSO): The division of Palm Beach State's Information Technology department that is responsible for the development of management, operational, and technical safeguards or counter measures prescribed for the information system to protect the confidentiality, integrity and availability of the system and its information.

Information Security Manger (ISM): Responsible to the Information Technology executive management for administering the information security functions within the College. The ISM is the College's internal point of contact for all information security matters.

Security Incident Response Team (SIRT): Personnel responsible for coordinating the response to computer security incidents in an organization

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, 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.

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.

Incident Management Procedure:

- Palm Beach State Information Technology Security Office (ITSO) will establish and provide overall direction to a Palm Beach State Security Incident Response Team (SIRT)
- Palm Beach State SIRT members have pre-defined roles and responsibilities which can take priority over normal duties.
- Palm Beach State ITSO will develop incident response procedures and test them on a regular basis
- 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 Palm Beach State ITSO is responsible for reporting the incident to the:

Information Security Incident Management

- ❖ Palm Beach State Executive Management
 - ❖ Any affected customers and/or partners
 - ❖ Local, state or federal law officials as required by applicable statutes and/or regulations
- The Palm Beach State ITSO is responsible for coordinating with the College Relations and Marketing department to establish all communications regarding the incident with all outside organizations.
 - All suspect activity including but not limited to possible security incidents must be reported to the Information Technology Assistance Center (iTAC – formally the helpdesk) immediately.

Enforcement:

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 volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Palm Beach State information resources access privileges, civil, and criminal prosecution.

Contact Information:

Questions, concerns or comments concerning this guideline should be directed to:

Tony Parziale

CIO

Palm Beach State College

4200 Congress Avenue, ITB 103

Lake Worth, Florida 33461

Tel: 561.868.3262

Fax: 561.868.3259

Revision History:

Version	Revision Date	Review Date	Description
1.0	6/30/2009	MM, DD, YYYY	