STATE BOARD OF PSYCHOLOGY OF OHIO
POLICY AND PROCEDURE MANUAL

SECTION 10: *ADMINISTRATIVE POLICIES AND PROCEDURES*

POLICY 10.10: I.T. SECURITY INCIDENT RESPONSE

PRIOR DATE EFFECTIVE: JULY 5, 2006

AMENDED AND EFFECTIVE: JULY 15, 2013

REVIEWED AND APPROVED:

Suzanne S. LeSure, Ph.D. _____ _____ 7/16/13
President Date Executive Director Date

Reference: DAS OIT Standard ITS-SEC-02

PURPOSE

The purpose of this policy is to establish IT security incident response (IR) capability relative to identified security incidents and to avoid said incidents. Security incidents are those adverse events that have been proven to be a verified IT security breach, examples of which are:

- Loss of confidential information
- Compromise of the integrity of information
- Loss of system availability
- Denial of Service
- Misuse of service, systems, or information
- Damage to systems from malicious attacks (e.g. viruses, Trojan horses or logic bombs)

Unauthorized system use and system crashes both might represent the first indicator of a security incident and this policy is intended to prevent such events and to establish procedures for recovery.

SCOPE

This policy applies to all of the State Board of Psychology's computers and equipment and its employees, contractors, temporary personnel and interns and other agents who use the Board's systems.

PROCEDURES

ADVERSE EVENT AND INCIDENT PREPARATION

1) **INCIDENT REPONSE TEAM.** There is hereby established an Incident Response Team (IRT), comprised of:

Ronald Ross, Executive Director
466-1085
ronald.ross@psy.ohio.gov

Bruce Sinmaz, IT Systems Analyst, Office of Information Technology (OIT)
752-9280
588-3598 cell/pager
bruce.sinmaz@das.ohio.gov

2) **RECOVERY PREPARATION.** To facilitate containment of adverse events and recovery following a security incident, the Board hereby establishes the following procedure:

Password Security: Employees shall safeguard all passwords that are required for access to secure systems. Passwords shall be updated according to procedures approved by the Executive Director, in consultation with the Office of Information Technology.

System Back-ups: Each employee or designee shall back-up critical systems and files on a semi-monthly basis by overwriting all critical information onto approved storage devices or backing up the information to the Board's dedicated space at the State of Ohio Computer Center.

3) **INCIDENT REPONSE PLAN**

Employees and others affected by the policy shall immediately report to the Executive Director and/or OIT (Bruce Sinmaz or designee) any adverse event. An adverse event is any observable occurrence in a system or network with negative consequences, such as:

- System crashes
- Unauthorized use of systems
- Defacement of the Board's web page
- Evidence of information alterations that appear malicious

Any report of an adverse event shall be investigated by OIT for evidence of an IT security incident, and staff shall be advised in office and/or through email as appropriate.

If an adverse event is determined to represent a security incident by OIT, staff shall follow directives from OIT and/or the Executive Director and shall cooperate in the collection of evidence, analysis, containment, and elimination of any threat. Information shall be documented by the Executive Director or designee and shall be safeguarded. In the event of an identified security incident, the event shall be documented and classified in conjunction with OIT. Any security incident shall be analyzed to determine if the event resulted in a breach of security of a system containing personal information as defined in ORC 1347.12 and then to notify affected individuals as required by ORC 1347.12.