INFORMATION SECURITY BREACH INCIDENT PLAN

I. PURPOSE

A. The Superintendent promulgates this regulation to ensure compliance with the in compliance with the Information Security Breach and Notification Act and BOCES policy.

B. All private information stored electronically should be on secure, BOCES approved information management systems. Employees having access to private information should understand their personal and professional responsibility for protecting student and employee information. Employees should be familiar with and review regularly Jefferson-Lewis BOCES Policy on acceptable use of BOCES' Systems.

II. Internal Notification

A. If a breach is suspected to have occurred personnel should concurrently immediately notify the Senior Administrator of their Department and the Security Breach Team Manager.

B. The Security Breach Team (SBT) shall be comprised of the following individuals:

1. Superintendent or his/her designee;
2. Security Breach Team Manager (SBT Manager);
3. Technical Support Staff; and
4. BOCES Legal Counsel.

III. Security Breach Team Roles and Responsibilities

A. A critical step in effective incident response is the SBT. The goal of SBT is to quickly and appropriately handle an incident. The SBT is responsible for implementing the information security breach policy, plan and procedures.

B. Superintendent or designee is responsible for:

1. Overseeing the entire response process;
2. Managing the overall response activities for all security incidents;
3. Decision-making regarding which courses of action will be taken; and
4. Determining when it is appropriate to share information outside the organization.

INFORMATION SECURITY BREACH INCIDENT PLAN

C. SBT Manager has the overall responsibility to ensure the implementation, enhancement, monitoring and enforcement of security policies and procedures.

The SBT Manager is responsible for:

1. Serving as the initial point of contact;
2. Notifying and briefing management as appropriate;
3. Accessing the situation and assisting in fixing the problem;
4. Providing options and recommendations to management on how to respond;
5. Coordinating activities and communicating within the incident response team; and
6. Developing and maintaining all documentation relating to the incident.

D. Technical Support Staff is responsible for:

1. Assessing the situation and providing recommendations to the SBT Manager;
2. Assisting the SBT Manager in gathering information;
3. Helping the SBT Manager in response and remediation;
4. Providing any other support to the SBT Manager and/or third party contractor utilized by BOCES as needed.

E. Legal Counsel will provide guidance and advice as appropriate.

F. Overview of roles in incident handling.

1. Identify: User identifies that there is a suspected security incident (all data users);
2. Notify: User notifies their teacher, supervisor, Department Administrator of the suspected security incident and Department Administrator notifies the SBT Manager;
3. Assess: SBT Manager assesses if the “security incident” is a “security breach” (SBT Manager).
4. Respond: Technical Support Staff respond to the “breach”.
5. Report: SBT Manager reports in accordance with the Incident Response Plan and Policy.
5. Review: SBT reviews of the overall effectiveness of the response procedures.

INFORMATION SECURITY BREACH INCIDENT PLAN

IV. Determining if a Breach Has Occurred

A. A determination of whether a breach has occurred will be made by the SBT Manager. A "security incident" may not rise to the level of a "security breach" and only the SBT Manager may make the determination if a "security breach" has occurred which would require a report in accordance with the Incident Response Plan.

B. In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or person without valid authorization, BOCES may consider the following factors, among others:

1. Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
2. Indications that the information has been downloaded or copied; or
3. Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or
4. System failures.

C. Possible causes of cyber incidents include the following:

1. Attempts to gain unauthorized access to a system or its data;
2. Unwanted disruption or denial of service (DoS);
3. Unauthorized access to critical computers, servers, routers, firewalls, etc.
4. Changes to system hardware or software without approval;
5. Virus or worm; or
6. Infection, spyware, malware.

D. Signs that a computer or system may have been compromised may include:

- Abnormal response time or non-responsiveness;
- Unexplained account lockouts;
- Inoperable passwords;
- Inability to open website homepage or unexplained changes/content to website;
- Programs not running properly;
- Lack of disk space or memory;
- Bounced back emails;
- Inability to connect to the network;

- Continuous or increasing crashes;
- Abnormal hard drive activity;
- Connecting to unfamiliar sites;
- Changes in browser settings;
- Extra or unfamiliar toolbars that cannot be deleted.

V. Investigation of Breaches

A. Breach investigations will be conducted by the SBT.

B. Steps to be taken in a breach investigation may include:

1. Determine exactly what information was compromised (i.e., names, addresses, contact information, social security numbers, student or employee ID numbers, credit/debit card numbers, grades, birth dates, passwords);
2. Take steps immediately to retrieve data and prevent any further disclosures;
3. Identity all affected records and students, employees and/or individuals;
4. Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised;
5. Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINs, etc.); storage; encryption; transmission; and destruction of information from education records;
6. Determine whether the incident occurred because of a lack of monitoring and oversight;
7. Conduct a risk assessment and identity appropriate physical, technological, and administrative measures to prevent similar incidents in the future;
8. Determine when the breach occurred;
9. Determine which computers or networks were involved;
10. Determine if the data encryption key was compromised;
11. Clarity the scope of the breach and the individuals involved (i.e., did it affect a specific, identifiable group of individuals on the District's network or was it random);
12. Determine if the breach also involved additional cyber incidents such as denial of service, scans or malicious code.

INFORMATION SECURITY BREACH INCIDENT PLAN

V. External Notification

A. If a determination has been made that a breach has occurred by the SBT then BOCES will then notify the New York State Attorney General (AG), the New York State Department Consumer Protection Board (CPB) and the New York State Office of Cyber Security (OCS), as required by law. Notification will occur using the form 4242-F - New York State Security Breach Reporting Form consistent with BOCES policy.

==========

Jefferson-Lewis-Hamilton-Herkimer-Oneida Board of Cooperative Educational Services
Legal Reference: NYS General Business Law §889-aa; NYS Technology Law §208, NYS Office of Cyber Security and Critical Infrastructure.
Approved by the District Superintendent: 06/21/17