Broward County Public Schools
Security Incident Handling Guidelines

Introduction and Overview

The School Board of Broward County, Florida is devoted to protecting the security and confidentiality of personal information. These guidelines address how the District will respond to the unauthorized access of computerized data (as well as data created and maintained in other formats) containing personal information.

Cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive. Theft of a laptop, desktop, mobile device or electronic media could result in a security attack. The BCPS Information Security Guidelines can lower the number of incidents, but not all incidents can be prevented. The following guidelines provide users with procedures for reporting computer security incidents and appropriate responses to each incident. The latest version of the security incident handling guidelines are posted to the Additional Links Section of the following website: http://www.browardschools.com/privacyinformation.

Data breach means an unauthorized or unlawful acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information, including but not limited to student information protected by the Family Educational Rights and Privacy Act (FERPA) and protected health information of employees or students as protected by the Health Insurance Portability and Accountability Act (HIPAA), maintained on District databases.

Incident Planning and Prevention

Broward County Public schools will plan for an incident by distributing the Security Incident Handling Guidelines, by establishing a Cyber Security Incident Response Team (CSIRT), and providing security awareness training to users. Prevention of incidents will be improved by user training in addition to the hardening of systems by protections such as firewalls, network security devices, antivirus, patches and other security best practices.

Data Breach Response Procedures

1. **Preserve the evidence.** Do not destroy any data or evidence related to the data breach and advise those involved to not destroy the data. This information will be needed to determine the scope of the breach and will be helpful in notifying affected individuals.
    a. If a suspected incident occurs on a user's mobile device, the user shall not turn off the device. The user will leave the device on and report the incident. A member of IT will look over the device and determine if the incident is contained to the one device.
2. **Inform appropriate staff.** Ensure prompt internal notification of appropriate persons when a breach is detected, including the use of an incident response team, management and the internal owner of the data.

a. **School or location administration**. If a user suspects a security incident, involving a BCPS **student**, the school or location administrator must be contacted immediately.
b. The school or location Administrator will contact the response team:
Special Investigative Unit (SIU) – (754) 321-0725
Privacy Officer (Risk Management Department) – (754) 321-1914
Manager of Information Security (I&T Department) – (754) 321-0411
Participation by different members of the response team may vary, depending on the nature of the incident. The response team will consult with the Office of the General Counsel as needed.
c. If a user suspects a security incident, involving BCPS **personnel**, a "Personnel Investigation Request" Form #4209 should be completed with the Special Investigative Unit (SIU).
d. If a user suspects a security incident, involving **non-personnel**, the "Immediate Notification Form" FORM #4617 should be completed with the Special Investigative Unit (SIU).

3. **Notify**. The response team will work with the Public Information Office (754-321-2300 / 754-321-2616) to develop talking points or a media response regarding the data breach, as needed.
4. **Investigate**. The response team will conduct an investigation, as applicable, and interview those involved, including suspected individuals and witnesses. Schools and locations shall cooperate during the investigation, including facilitating access to pertinent individuals and a private setting to conduct the interviews.
5. **Assess nature and scope**. The response team will work together with school/department based administration to assess the nature and scope of the incident, and identify the systems and personal information that has been accessed or misused. Sample questionnaire:
    a. Was data downloaded from SAP or TERMS or other district system onto the hard disk of the device?
    b. If so, did the data include Social Security numbers or any data that could lead to identity theft?
    c. Did the data include any items that are not considered public record – such as medical information of staff or students?
    d. Was the data a subset of employees/students or all?
6. **Contain, control and correct.** The response team will contain, control and correct any security incidents while documenting all responsive actions taken. Certain information collected during the course of an investigation may be temporarily designated as confidential to prevent the risk of deletion of forensic evidence.
    a. Locate, obtain, and preserve all written and electronic logs and records applicable to the breach for examination
    b. Remove access to the data from those suspected of being involved in the breach. Under no circumstances should data nor evidence related to the incident be destroyed.
    c. If a suspected incident occurs on a user's mobile device, do not turn off the device. Plug device to proper power supply to maintain powered on state.
    d. Document the source/cause of the incident (if known), including usernames, hostnames and IP addresses
    e. Describe the effected resources (ex: networks, hosts, applications, data), including systems' hostnames, IP addresses, and function
    f. Document method of attack associated with the incident (if known), and indicators related to the incident (ex: content engine logs, filter logs, system logs, traffic patterns, registry keys, etc.).

g. Document actions taken by all incident handlers and response team members. Example Actions:
    1. Patched/Ran Antivirus scan and cleaned infected device
    2. Removed source machine from network (shutdown port/shutdown device)
    3. Disabled user account / Changed user password
    4. Fixed permissions

7. **Notify**. Contact individuals affected by a breach of their data as required by federal and/or state law. When notification is required, different Florida Statutes and federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA) impose timeframes for breach notifications (to victims). Therefore internal notification to appropriate District staff (the response team) in a timely manner is vital.
    a. In the event that personal information was, or is reasonably believed to have been, acquired by an unauthorized person, notification to the victim shall be made without unreasonable delay.
    b. Notification shall comply with Florida Statue 501.171 and/or HIPAA regulations.
    c. The response team will assist the school or department in preparing the notification to be distributed by the school or department administration to the affected individual(s) as well as any recommended notices / directives to unintended recipients (when applicable).
8. **Review**. The response team will regularly review and update the incident response plan as necessary
9. **Increase staff awareness.** Advise employees on the importance of protecting confidential information and immediately reporting breaches.

Attack Methods

The following are some examples of attack methods that may result in security incidents:

1. Improper Usage: User violation of the BCPS acceptable usage policies and information security guidelines.
2. Loss or Theft: The loss or theft of a computing device or media, such as a laptop or smartphone.
3. External/Removable Media: An attack executed from removable media (ex: flash drive, CD)
4. Attrition: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.
5. Web: An attack executed from a website or web-based application.
6. Email: An attack executed via an email message or attachment.

Incident Examples

The following are examples of some incidents that users may encounter and that may need to be reported.

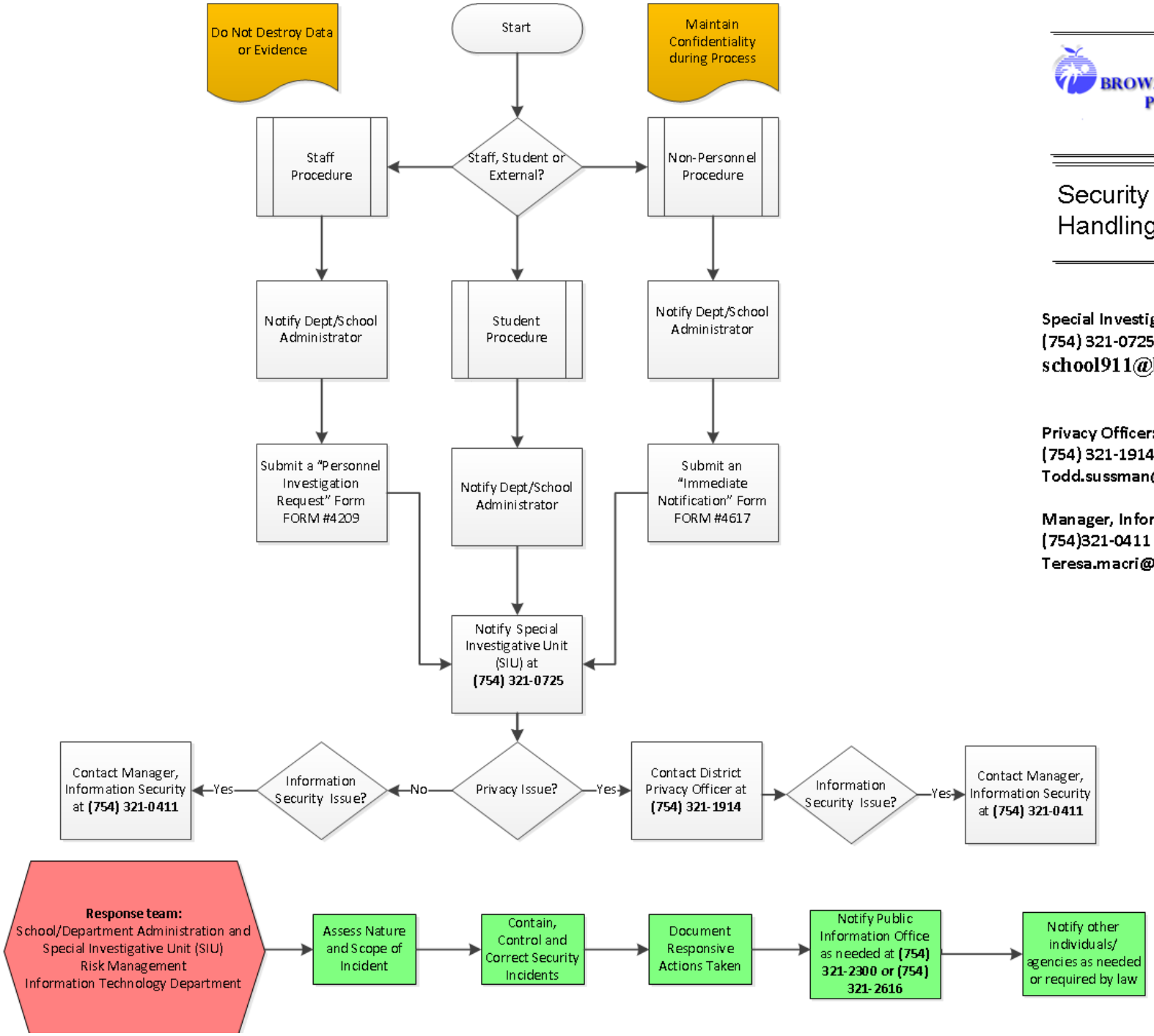
1. A user is suspected of accessing a system for which he/she is not authorized with malicious intent. (Student Information System, Gradebook, District server, website, etc.)
2. A user provides or exposes sensitive information to others. (Social Security Numbers, etc.)
3. An attacker uses a hacking tool to gain entry into systems and or cause a denial of service or otherwise inhibiting normal use of the system.
4. User tricked into opening an attachment/link that is actually malware; running the tool has infected their computer and established connections with an external host.
5. A user loses a mobile device either by theft/loss which contains BCPS email or other data

Incident Tickets

1. If the Information and Technology Department and/or the BCPS Network Operations Center suspect that an incident has occurred, they should immediately start recording all facts regarding the incident on a Remedy ticket.
2. If the Special Investigative Unit (SIU) contacts Information and Technology Department and/or the BCPS NOC for assistance in an investigation, a remedy ticket should be generated.
3. Remedy ticket should include description of evidence documented by response team and used to track the progress of the detection, analysis, containment and recovery of the security incident.

References:

http://www.nist.gov
http://www.sans.org
BCPS Information Security Guidelines
BCPS "School and District Technology Usage" policy: Policy 5306
Family Educational Rights and Privacy Act (FERPA)
Florida Statue 501.171 "Security of confidential personal information."
Health Insurance Portability and Accountability Act (HIPAA)
NIST Policy 600-04, Standard 600-04S1, 800-53 and 800-61



BROWARD COUNTY PUBLIC SCHOOLS

Security Incident Handling Guidelines

Special Investigative Unit (SIU):
(754) 321-0725
school911@browardschools.com

Privacy Officer:
(754) 321-1914
Todd.sussman@browardschools.com

Manager, Information Security:
(754)321-0411
Teresa.macri@browardschools.com