Tim Forson
Superintendent of Schools

40 Orange Street
St. Augustine, Florida 32084
(904) 547-7500
www.stjohns.k12.fl.us

MANAGEMENT DIRECTIVE 5.03

Revision 4

DATE: December 1, 2017

TO: All Employees

FROM: Tim Forson, Superintendent

SUBJECT: Computer Security Procedures/Practices/Resources

This directive outlines employee responsibilities needed to safeguard the District's information systems data integrity and confidentially, systems reliability, digital resources and system operation. Employees are required to support this mission by reporting security incidents, safeguarding their system access, becoming knowledgeable on computer security practices and helping others (including students) with the same. This directive highlights the most significant computer security documents and resources applicable to employees.

1. Computer Security Incident

In general terms, a computer security incident involves the damage/loss or the deliberate interruption of service to computer systems, unauthorized release of confidential data, unauthorized access, and/or compromise of system data, reliability or integrity or violation of state or federal laws related to information security.

If an employee suspects, witnesses or has knowledge of a Computer Security Incident that involves District Network/Computer systems or data (staff/student) they are to perform the following action (excerpt from the Computer Security Incident Response Plan (CSIRP):

1. Within (1) day or upon incident or suspected incident discovery perform the following:

   During working hours:

   a) Call the IT Department administration at (904) 547-3920 or the IT Help Desk at (904) 547-HELP and provide a real-time report of the concern or incident. If an incident has occurred, submit a Web Ticket navigating to ***Computer Security Incident*** and complete the Security Incident Questionnaire.

   After working hours:

   c) When a computer security concern or incident occurs after hours, please explain the situation and any pertinent details in an email to Security@stjohns.k12.fl.us. Provide a phone number where you can be reached for further clarification. Submit a Web Ticket navigating to ***Computer Security Incident*** and complete the Security Incident Questionnaire.

For more detail, please reference the Computer Security Incident Response Plan (CSIRP) that can be found on the InsideSJCSD website under the IT Department, Security Awareness.

2. Security Awareness Program

The IT Department publishes ***Security Awareness Notes*** throughout the year to promote our Security Awareness Program. The goal of this program is to educate all users of the St. Johns County School District's digital network and users of the District's corporate information systems or resources of proper security practices and procedures. All Security Awareness Notes can be accessed via the InsideSJCSD website under the IT Department.

Security Awareness Notes highlight areas of concern and explain new procedures. They also provide guidance and/or additional procedures related to the use of the network, digital security, emerging trends, security concerns and new IT initiatives as they are developed. Each employee is expected to read and comply with each Security Awareness note as it applies to use of the network and its resources. The most impactful topics covered by Security Awareness Notes include:

a. Network Password Rules and Changes
b. Network check-in Procedures
c. Webcam Administration
d. Procedures for Handling Sensitive Data
e. Remote Access
f. Computer Check-out forms

If you have any questions about this topic, or the Security Awareness Program in general, please contact our Security Specialist at Security@stjohns.k12.fl.us or ext. 13971. Annual employee training focused toward District Computer Security procedures and practices is being developed in the 2015-16 SY which will be posted on the InsideSJCSD.

3. Acceptable Use Procedures (AUP)

The AUP is divided into two categories, Students/Visitors and Employees/Staff. The AUP outlines the proper uses and unauthorized uses of the District's Digital Network. All users of the SJCSD Digital network and/or resources must read and acknowledge the applicable AUP each school year. The signed forms are to reside in each school or department. The District Website is the easiest place to reference the applicable AUP documents and forms, http://www.stjohns.k12.fl.us/it/aup/.

- For Students and Visitors:
  - Students and Visitor AUP
  - Student AUP Agreement Form

- For Employees:
  - Board Rule 6.83 (AUP for Employee use of District Electronic Systems)
  - Management Directive 5.01 (Employee AUP Procedures)
  - Employee AUP Agreement Form
  - Employee Technology Device Terms and Use Conditions
  - Employee Technology Equipment Responsibility Form
  - Employee Technology Device Damage or Loss Report Form

4. Computer-related School Board Rules

The following School Board rules provide policy related to computer use or security and can be found on the District Website under School Board:

- 6.82 Use of Electronic Media for School Purposes
- 6.83 Employee AUP (with key elements outlined in section 3 above)
- 6.84 Employees' Use of Social Network Websites

5. Other Management Directives related to Computer Use and Security

The following Management Directives provide procedure related to computer use or security and can be found on the District's InsideSJCSD Website for employees:

- 5.04 Use of Social Networking Websites & Other forms of Public Broadcasting This revision supersedes previous versions. If you have any questions, please contact the Information Technology Department at extension 13920 or the Help Desk at 547-HELP.