TOLLAND PUBLIC SCHOOLS
Tolland, Connecticut

ADMINISTRATIVE REGULATION

REGARDING: ELECTRONIC INFORMATION SECURITY

Number: 4111
Personnel

Approved: 12/11/13

The school system will maintain access management processes to ensure that appropriate access will be afforded to electronic information resources.

Controlling access to electronic information, systems and security:

A. Managing access control standards

Access control standards for information systems and infrastructure will be established and maintained by district information technology (i.t.) management and the superintendent to incorporate the need to balance protection from unauthorized access and data loss with the need to provide access to meet legitimate district or curriculum objectives.

B. Managing user access

Access to all district systems, networks and infrastructure must be authorized by the district i.t. staff. Such access, including the appropriate access rights (or privileges) must be documented. Such documentation is to be regarded as confidential and safeguarded accordingly.

C. Securing unattended workstations and equipment

All district equipment, or personal equipment attached to district networks or infrastructure, are to be safeguarded appropriately – especially when left unattended. It is each individual user's responsibility to ensure the equipment is secured with password protection for authentication when left unattended. Password authentication is required for all connected systems in the case of user/system "time out".

D. Managing network access controls

Access to the resources on the network will be controlled by district i.t. Staff to prevent unauthorized access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized.

E. Administrative rights to systems, networks, and infrastructures

Administrator rights access to systems, networks and infrastructure will be restricted to only district i.t. staff. The purpose of this policy is to ensure that appropriate system management, security, and licensing standards are maintained and documented. The superintendent request administrator rights be granted to individual systems after a documented business need is identified and agreed to by the district i.t. staff.

F. Controlling access to operating system software

Access to operating system commands, such as application installation, is to be restricted to district i.t. staff who are authorized to perform systems administration/management functions.

G. Managing passwords

The selection of passwords, their use and management as a primary means to control access to systems must strictly adhere to best practice guidelines provided by district i.t. staff. In particular, personal account/device passwords shall not be shared with any other person for any reason. System passwords will be changed every 90 days.

H. Securing against unauthorized physical access physical access

Designated high security areas are to be controlled with strong identification and authentication techniques. Staff with authorization to enter such areas are to be provided with information on the potential security risks involved.

I. Monitoring system access and use

Access to information systems, networks and infrastructure is to be logged and monitored to identify potential misuse of systems or information by district i.t. staff

J. Controlling remote user access

Remote access control procedures, managed by district i.t. staff, will provide adequate safeguards through robust identification, authentication and encryption techniques.