SECTION V: BUSINESS AND TECHNOLOGY POLICY 5020

Information Technology

Information Technology

The Information Technology policies established below are applicable to everyone (All employees, teachers, contractors and vendors must ensure compliance) accessing K12 systems or utilizing technology assets.

Access to Systems

User provisioning / de-provisioning requirements.

- Notification of termination or changes in roles must be communicated to K12Corporate Human Resources and the Regional Technology Manager on or before the termination for removal/ change of access. This includes all employees, co-employees (i.e., Insperity) and contractors).
- Timely revocation of accounts must occur for all systems a terminated user has access to or as a role changes occur.
- Documented approval of new user access must be obtained from the Head of School.
- Laptops / workstations must be returned immediately to Regional Technology Manager upon staff termination.

Semi-annual user appropriateness review, intended to validate appropriate user access and identify accounts that should be deactivated due to terminations and must be completed within two weeks of receiving request. Review results must be approved by the Head of School.

Password Protection

All employees, teachers, contractors and vendors accessing K12 systems must adhere to the following password policy:

- Minimum of 8 characters
- 3 out of 4 complexity factors (uppercase, lowercase, special character and numbers)
- Not consist of readily known information or common words
- Changed every 90 days
- Be concealed upon entry (not visible when typed into application)
- Not be shared
- Changed immediately if compromised

Physical Security

Laptops must be secured via a cable lock or other similar device, while stationary devices will rely on physical / facility security measures. Physical security will be applied to central computer installations, office environments and 3rd party hosted facilities. Access is limited to required personnel through locked door or badged access

Source: OVCA Board Policy adoption 11/17/2016

Data Security

Appropriate encryption should be established for exchange of protected information.

- Documents stored outside of protected systems (i.e., flash drives and other media) must be secured with a password or encrypted
- Personally identifiable information (i.e., social security numbers, credit cards, student information) should limited and generally not sent through a public domain e-mail system (i.e., Hotmail, Yahoo, Google)

Virus protection must be applied on all computers and servers

- Protection must be configured to run automatically
- Virus definitions must be up to date.

System Development and Changes

All system development (including hosted applications) must be performed in an environment separate from production and changes into production must be controlled, documented and approved.

- Changes must be tested outside of the production environment and confirmed by system owner prior to implementation.
- Changes deployed into production must be verified by the system owner with documented review approval.

Default passwords for vendor provided applications are changed upon implementation.

Source: OVCA Board Policy adoption 11/17/2016