DATA GOVERNANCE AND SECURITY
(Account Management)

The information security officer (ISO) will implement the following procedures for granting, modifying and terminating access to the district's network or confidential or critical district information. Such access is a privilege, not a right, and access may be terminated by the ISO at any time for any legal reason.

Granting User Access

User access will be based solely on whether the individual needs access to the information and will not be based on the person's position in the district or title. For example, even the superintendent will not necessarily have access to all information in the district at all times if such access is not necessary to perform his or her job responsibilities.

The human resources department will notify the ISO when an employee is assigned to a new position or given additional duties and will work with the ISO or designee to determine the appropriate level of employee access to confidential or critical information.

Departments that engage independent contractors, vendors or volunteers who need to access the district's network or secure files must contact the ISO. Contractors, vendors and volunteers will be granted access to the district's network or secure files only after agreeing in writing to maintain the confidentiality and security of the information and follow the district's policies, procedures and security rules. Access will be limited to the information the contractor, vendor or volunteer needs and will be terminated after a specific period of time.

Students may be granted access to limited portions of the district's network. The ISO will work with building principals to determine the extent of the access.

Requests for Greater Access

A user who desires greater access than has been granted must contact the ISO to request a change of credentials. Access will not be granted unless the user demonstrates a need to know the information, as determined by the ISO in consultation with the employee's supervisor.

The ISO will keep records of level of access by role or position and records of any exceptions made when additional access is needed by a user. These records will be updated regularly.

Alternate or Emergency Access

District employees who work with critical business functions or confidential information are encouraged to designate one or more alternate employees who will perform those functions in their absence or in an emergency situation. The ISO will document these designations so that the alternate is given the necessary access immediately upon notification that access is needed.

User Identification and Password Requirements

The district will require all users to have a unique user identification and a secure password before accessing confidential or sensitive district information. The district will require strong password controls of appropriate length and complexity and will prevent users from relying on previously used passwords. The district will utilize the district's network management system to enforce those requirements.

Passwords necessary to access district confidential or critical data will be changed at least every 120 days. Passwords to access other district data will be changed at least every six months. Users are prohibited from sharing their user identifications and passwords with others or using another person's user identification and password.

Resetting Lost or Compromised Passwords

Users and employees who have reason to believe a password is lost or compromised must notify the ISO or designee as soon as possible. The technology department will verify the identity of the person requesting the change before resetting the password.

Terminating User Access

When short-term users (such as substitute employees, vendors and independent contractors) are provided access to the district's network, the ISO or designee will document a date when access will end, if possible, or document a date when the ISO or designee will inquire about continued access.

The human resources department will notify the ISO or designee when an employee resigns or is terminated, put on administrative leave or deemed to be a security risk. Once notified, the ISO or designee will terminate the employee's access on the appropriate effective date.

Students will generally be given continued, limited access to the district network until they graduate from the district. District principals or their designees will notify the ISO or designee when a student withdraws, transfers, graduates, is put on a long-term suspension, has lost technology privileges, or is deemed to be a security risk. The ISO or designee will terminate the student's access on the appropriate effective date.

Monitoring and Reviewing Access

At least annually, the ISO or designee will audit user access to verify that the information a user has access to is appropriate given the user's position. Based on the review, access rights may be added, changed or removed.

Monitoring Inactive Accounts

The ISO or designee will routinely review account access logs for unusual activity or inactivity. If an employee has been given access to an area but has not accessed information from that area for more than a year, the ISO will consult with the employee's supervisor to determine whether access is still needed.

Concurrent Access

The ISO or designee will ensure that the district uses software controls, when available, to restrict concurrent access to district systems so that a single user can access the district's information system at only one location at any given time.

* * * * * * *

Note: The reader is encouraged to review policies and/or forms for related information in this administrative area.

Implemented: November 29, 2017

Revised:

Boonville R-I School District, Boonville, Missouri