DATA GOVERNANCE AND SECURITY
(Security Controls)

Logical Security Controls

The district will use logical security controls, such as user identification and password access, user authentication, access rights and authority-level protocols, to maintain the security of the district's confidential and critical information. The district will use defenses to protect against viruses, malware, spyware, phishing and spam. Users are prohibited from turning off or disabling district protection systems.

Physical Security Controls

The district will use physical security controls to maintain the security of the district's confidential and critical information. The information security officer (ISO) will create and maintain physical security controls that protect district servers, network routers and essential network equipment from unauthorized access or theft and damage from fire, water, extreme temperature changes and power outages. The ISO will create locked, physical barriers to this equipment, such as locked doors or cages.

The ISO will determine who will be allowed access to essential district equipment. Those with authorized access will be provided keys or access codes to the physical barriers. The keys and access codes cannot be shared without the ISO's permission, and the ISO must be notified immediately if the keys or access codes have been compromised. The district will record who accesses essential district equipment, electronically or otherwise, using appropriate security devices, such as keys, electronic key logs, security cameras or other appropriate measures.

The ISO may temporarily grant access to a vendor or other person when determined necessary. The name of the person, the reason for the access and the date and time of the access will be documented, and the ISO will determine whether the person needs to be accompanied by district staff before access is granted.

Physical records that include critical and confidential information will be stored in locked cabinets or in rooms with limited access. The superintendent or designee will determine who will have access to these records and will distribute keys or access codes.

Security Logs

The ISO will identify the types of security events the district will log and monitor and will ensure that the district's network management system's logging settings are appropriately used. The district's incident logs will include appropriate information so that the district can monitor significant

system events. At a minimum, the district will log access to sensitive or critical system resources or information, data breaches and compromised account credentials.

Security Audit

The ISO or designee will regularly audit the district's security controls and make adjustments as necessary. All audits will be documented.

Business Continuity and Data Recovery Plan

Backing Up Data

The ISO will create a process by which critical district data will be backed up and stored in more than one location, and one such location must be off district property or in a different building. The ISO will ensure that the backup data is tested and validated to ensure that the backup is occurring and information can be restored. The ISO has identified the following information as critical:

- *Student information system database and servers*
- *Financial and HR system database and servers*
- *Email Server*
- *Library card catalog*
- *Fileserver*

Alternative Data-Processing Site

Some events, such as a tornado or flood, prevent the district from using its own equipment to restore or process backed-up data. For that reason, the district has designated an offsite server hosted in Kansas City, MO as its alternative data-processing site.

The ISO and designated employees will be trained in how to restore data using the alternative data processing site.

Restoring Critical Systems and Data

If an event occurs that prevents district staff from accessing critical information, the ISO or designee will access and restore the backup data. Because it will take time to restore massive amounts of data, unless the ISO determines otherwise, data will be restored according to a restore priority spreadsheet maintained by the district technology staff.

Testing Continuity Plan

The ISO and designated staff will routinely test the district's continuity plans to ensure that they are effective, to identify weaknesses in the plan, and to ensure that designated staff have received adequate training.

* * * * * * *

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

Implemented:

Revised:

Boonville R-I School District, Boonville, Missouri