Definitions and Responsibilities
Appendix C

Definitions

A. **Availability:** Data or information is accessible and usable upon demand by an authorized person.
B. **Confidentiality:** Data or information is not made available or disclosed to unauthorized persons or processes.
C. **Customers:** Staff, parents, employees (including contract), and students are considered customers of the school district.
D. **Data:** Facts or information
E. **Information:** Knowledge that you get about something or someone; facts or details.
F. **Data Integrity:** Data or information has not been altered or destroyed in an unauthorized manner.
G. **Involved Persons:** Every user of Involved Systems (see below) at Mountain Brook Schools – no matter what their status. This includes nurses, residents, students, employees, contractors, consultants, temporaries, volunteers, substitutes, student teachers, interns, etc.
H. **Involved Systems:** All data-involved computer equipment/devices and network systems that are operated within the Mountain Brook Schools physical or virtual (cloud) environment. This includes all platforms (operating systems), all computer/device sizes (personal digital assistants, desktops, mainframes, telephones, laptops, tablets, game consoles, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.
I. **Personally Identifiable Information (PII):** PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
J. **Risk:** The probability of a loss of confidentiality, integrity, or availability of information resources.

Responsibilities

A. **Data Governance Committee:** The Data Governance Committee for Mountain Brook Schools is responsible for working with the Information Security Officer to ensure security policies, procedures, and standards are in place and adhered to by entity. Other responsibilities include:
    1. Reviewing the Data Governance and Security Policy annually and communicating changes in policy to all involved parties.

2. Educating data custodian and user management with comprehensive information about security controls affecting system users and application systems.

B. Information Security Officer: The Information Security Officer (ISO) for Mountain Brook Schools is responsible for working with the superintendent, data governance committee, user management, owners, data custodians, and users to develop and implement prudent security policies, procedures, and controls. Specific responsibilities include:

1. Providing basic security support for all systems and users.
2. Advising owners in the identification and classification of technology and data related resources.
   See also Appendix D (Data Classification.)
3. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
4. Performing or overseeing security audits.
5. Reporting regularly to the superintendent and Mountain Brook Schools Data Governance Committee on Mountain Brook Schools' status with regard to information security.

C. User Management: Mountain Brook Schools' administrators are responsible for overseeing their staff use of information and systems, including:

1. Reviewing and approving all requests for their employees' access authorizations.
2. Initiating security change requests to keep employees' secure access current with their positions and job functions.
3. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.
4. Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.
5. Providing employees with the opportunity for training needed to properly use the computer systems.
6. Reporting promptly to the ISO the loss or misuse of Mountain Brook Schools' information.
7. Initiating corrective actions when problems are identified.
8. Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any technology or data system/software to manage information.
9. Following all privacy and security policies and procedures.

D. Information Owner: The owner of a collection of information is usually the administrator or supervisor responsible for the creation of that information. In some cases, the owner may be the primary user of that information. In this context, ownership does not signify proprietary interest, and ownership may be

shared. The owner may delegate ownership responsibilities to another individual by completing the Mountain Brook Schools Information Owner Delegation/Transfer Request Form and submitting the form to the Data Governance Committee for approval. The owner of information has the responsibility for:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on ALSDE guidelines, industry standards, data governance committee guidelines, or advice from the school system attorney.
3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created.
4. Authorizing access and assigning data custodianship if applicable.
5. Specifying controls and communicating the control requirements to the data custodian and users of the information.
6. Reporting promptly to the ISO the loss or misuse of Mountain Brook Schools' data.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
9. Following existing approval processes within the respective organizational unit and district for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

C. **Data Custodian:** The data custodian is assigned by an administrator, data owner, or the ISO based his/her role and is generally responsible for the processing and storage of the information. The data custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:

1. Providing and/or recommending physical safeguards.
2. Providing and/or recommending procedural safeguards.
3. Administering access to information.
4. Releasing information as authorized by the Information Owner and/or the Information Privacy/ Security Officer for use and disclosure using procedures that protect the privacy of the information.
6. Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO.
7. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
8. Reporting promptly to the ISO the loss or misuse of Mountain Brook Schools data.
9. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

D. **User:** The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

1. Access information only in support of their authorized job responsibilities.

2. Comply with all data security procedures and guidelines in the Mountain Brook Schools Data Governance and Use Policy and all controls established by the data owner and/or data custodian.
3. Keep personal authentication devices (e.g. passwords, secure cards, PINs, access codes, etc.) confidential.
5. Report promptly to the ISO the loss or misuse of Mountain Brook Schools' information.
6. Follow corrective actions when problems are identified.