This guideline establishes the minimum requirements and responsibilities for data backup within Minnesota State Colleges and Universities (system). Institutions must apply local operational procedures to ensure timely backup of critical data - i.e. data that needs to be preserved in support of the institution's ability to recover from a disaster or to ensure business continuity.

This guideline applies where backups are required by the system, or institution policy or procedure. This guideline covers information technology resources, such as computer equipment or storage media, and other electronic media that may contain critical data. It also covers any

Removable backup media taken offsite must be stored in an offsite location that is insured and bonded or in a locked media rated, fire safe.

Removable backup media kept onsite must be stored in a locked container with restricted physical access.

See System Guideline 5.23.1.3 Data Sanitization.

Non-public data stored on removable backup media must be encrypted. Non-public data must be encrypted in transit and at rest when sent to an offsite backup facility, either physically or via electronic transmission. Refer to System Guideline 5.23.1.2 Encryption for Mobile Computing and Storage Devices.

Third parties' backup handling & storage procedures must meet system, or institution policy or procedure requirements related to data protection, security and privacy. These procedures must cover contract terms that include bonding, insurance, disaster recovery planning and requirements for storage facilities with appropriate environmental controls.

An archive is a collection of historical data specifically selected for long-term retention and future reference. It is usually data that is no longer actively used, and is often stored on removable media.

A copy of data that may be used to restore the original in the event the latter is lost or damaged beyond repair. It is a safeguard for data that is being used. Backups are not intended to provide a means to archive data for future reference or to maintain a versioned history of data to meet specific retention requirements.

Data that needs to be preserved in support of the institution's ability to recover from a disaster or to ensure business continuity.

Information collected, stored, transferred or reported for any purpose, whether in computers or in manual files. Data can include: financial transactions, lists, identifying information about people, projects or processes, and information in the form of reports. Because data has value, and because it has various sensitivity classifications defined by federal law and state statute, it must be protected.

Destruction of media includes: disintegration, incineration, pulverizing, shredding, and melting. Information cannot be restored in any form following destruction.

A safe designed to maintain internal temperature and humidity levels low enough to prevent damage to CDs, tapes, and other computer storage devices in a fire.

A statement that is optional.

A statement that is required for a compliant implementation.

Acceptable amount of service or data loss measured in time. The RPO is the point in time prior to service or data loss that service or data will be recovered to.

Acceptable duration from the time of service or data loss to the time of restoration.

A statement that is recommended but not required.

Referring to the Board of Trustees, the system office, the state colleges and universities, and any part or combination thereof.

Board policies 1A.1 and 5.23 delegate authority to the vice chancellor to develop system guidelines, consistent with Board policy and system procedure, for the purposes of implementing Board policy 5.23.