Guideline 5.23.1.11 Data Backup

Part 1. Purpose. 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.

Part 2. Applicability. 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 third party that hosts critical data. This guideline establishes requirements for data backup, and it is not intended to support data archival for future reference or to maintain a versioned history of data. Institutions may adopt additional requirements, consistent with this guideline and Board policy 5.23, for information technology resources under their control.

Part 3. Guidelines.

Subpart A. Local Data Backup Procedures. The institution must define local data backup procedures to support the institution's requirements to preserve critical data. The data backup procedures must include frequency, data backup retention, testing, media replacement, recovery time, and roles and responsibilities. Local data backup procedures must include the following:

1. **Frequency.**
    a) Primary backup: The recovery point objective (RPO) must be no earlier than the end of the previous business day.
    b) Offsite backup: Institutions must maintain a monthly full backup offsite at a minimum of 7 miles from their primary data center. Institutions should also maintain weekly backups at the same offsite location. The RPO for offsite backups must be no more than 35 days prior to the loss or corruption of data.
2. **Data Backup Retention.** Retention of backup data must meet system and institution requirements for critical data.
3. **Testing.** Restoration of backup data must be performed and validated on all types of media in use at least every six months.
4. **Media Replacement.** Backup media should be replaced according to manufacturer recommendations.
5. **Recovery Time.** The recovery time objective (RTO) must be defined and support business requirements.
6. **Roles and Responsibilities.** Appropriate roles and responsibilities must be defined for data backup and restoration to ensure timeliness and accountability.

7. **Offsite Storage.** 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.
8. **Onsite Storage.** Removable backup media kept onsite must be stored in a locked container with restricted physical access.
9. **Media Destruction.** See System Guideline 5.23.1.3 Data Sanitization.

Subpart B. Encryption. 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.

Subpart C. Third Parties. 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.

Part 4. Definitions.

Subpart A. Archive. 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.

Subpart B. Backup. 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.

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

Subpart D. Data. 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.

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

Subpart F. Media Rated, Fire Safe. 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. Safes are rated based on the length of time the contents of a safe are preserved while directly exposed to fire and high temperatures.

Subpart G. Information Technology Resources. Facilities, technologies, and information resources used for system information processing, transfer, storage, and communications. Included in this definition are computer labs, classroom technologies, computing and electronic communications devices and services, such as modems, e-mail, networks, telephones (including cellular), voice mail, fax transmissions, video, multimedia, and instructional materials. This definition is not all-inclusive, but rather, reflects examples of system equipment, supplies and services.

Subpart H. Institution. A system college or university, the system office, or the system as a whole.

Subpart I. May. A statement that is optional.

Subpart J. Must. A statement that is required for a compliant implementation.

Subpart K. Recovery Point Objective (RPO). 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.

Subpart L. Recovery Time Objective (RTO). Acceptable duration from the time of service or data loss to the time of restoration.

Subpart M. Should. A statement that is recommended but not required.

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

Part 5. Authority. 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.

Date of Adoption: 10/25/10,
Date of Implementation: 01/25/12,

Date and Subject of Revision:

1/25/12 – The Chancellor amends all current system procedures effective February 15, 2012, to change the term "Office of the Chancellor" to "system office" or similar term reflecting the grammatical context of the sentence.