Policy title	Category
Data Security Principles Policy	Administration Human Resources Information Technology Student Conduct
Owner	**Approved by**
CS/IT	Ad Council

Policy statement

Nebraska Wesleyan adopts the following principles for the privacy and security of data in its possession:

1. General Statement. It is the policy of Nebraska Wesleyan University to exercise reasonable care, in view of the state of technology as it currently exists, to maintain the privacy and security of all data in its possession.
2. Minimum Necessary Access. Nebraska Wesleyan University will establish and maintain physical, administrative and technical safeguards to see that that information in the possession of the University is accessible only by those persons who reasonably require such access in the exercise of their assigned duties.
3. Vendor Compliance: Nebraska Wesleyan University will require any vendor, supplier or other third party to adhere to the principles set forth in this Policy, to the extent these third parties are in possession of data regarding individuals associated with Nebraska Wesleyan University.
4. Encryption. Nebraska Wesleyan University will encrypt data at rest and in motion. Nebraska Wesleyan's use of unencrypted email will be limited to only those matters that do not involve information about individuals associated with the University. Nebraska Wesleyan University will require full-device encryption, wireless network encryption, and encrypted file transfer wherever feasible.
5. Backups. Nebraska Wesleyan University will establish and maintain a continuous backup regime for all information stored by the University, and prepare itself to resume business operations in the event of a catastrophic failure of its information systems within a commercially reasonable time frame.
6. Physical Security. Where Nebraska Wesleyan University maintains data centers, mainframe computers, or other large-scale computing facilities, Nebraska Wesleyan will provide reasonable physical security to such facilities, including, where feasible, access control and logging.
7. Disposal. Nebraska Wesleyan University will create, publish and maintain procedures for the secure deletion of data no longer needed for the University's operation, and for the secure destruction of storage media such as paper documents, hard drives and optical disks.
8. Training. No less often than annually, Nebraska Wesleyan University will train all faculty and staff on the current legal requirements associated with the collection, storage and processing of data about individuals, to a degree appropriate for the job duties of each person. Such training will include practical education on recognizing and avoiding the risks of inadvertent disclosure of protected information, such as by social engineering or malware.
9. Monitoring. The University will acquire and operate such logging and monitoring technology as may be necessary to provide itself reasonable assurance that University policies are being complied with and its computing resources are secure from unauthorized use. This includes, but is not limited to, anti-malware and intrusion detection technology.
10. Access Control. The University will require industry-standard access control measures, including passwords of adequate strength and, where appropriate, multi-factor authentication, for all computing resources.
11. Patch Management. Nebraska Wesleyan will provide for the prompt application of trusted security updates to all University computing resources, in order to maximize the security of those resources.

12. Auditing and Testing. The University will periodically enlist the assistance of third parties to assess the adequacy of this policy and the University's compliance with it.
13. Mobile Device Management. The University will use reasonable technological controls to assure that only devices owned or operated by authorized persons are allowed to access University network resources.
14. Administrative credentials. Not more than one person may use any credential, password, login, or other access control in order to perform system administration duties. Each such person is responsible for acts committed with his or her credentials.
15. Security Incidents. Should any person know or reasonable suspect that unauthorized use of, or access to, University systems or networks has occurred or may occur, that person must promptly notify a member of the senior leadership of the University not suspected of involvement in the incident. The University will promptly investigate any suspected security incident and discharge any legal obligation associated with it.
16. Business Continuity. The University will develop and maintain procedures for investigating, responding to, and recovering from any loss of data or computing services within a commercially reasonable time frame.
17. Insurance. The University will obtain a reasonable amount of insurance coverage for reasonably foreseeable losses related to technology.
18. Annual Review. At least once per year, a person designated by the President will review this policy, assess Nebraska Wesleyan University's compliance with it, and recommend to the President (a) measures to secure further compliance, and (b) changes to the policy necessary to keep data private and secure.

Approved by Ad Council 3/23/21

Last revised date March 23, 2021