Policy title	Category
Information Security Policy	Administration Information Technology
Owner	**Approved by**
ITS	Ad Council

Purpose of this policy

Nebraska Wesleyan University ("University") has adopted the following Information Security Policy as a measure to protect the confidentiality, integrity and availability of Institutional Data as well as any Information Systems that store, process, or transmit Institutional Data.

Application of this policy

This policy applies to all Nebraska Wesleyan University Information Technology Services (ITS) standards and university technology assets. Any information not specifically identified as the property of other parties, that is transmitted or stored on Information Systems (including email, messages, and files), shall be considered the property of The University and to which this policy applies. However, this policy does not supersede the rights and ownership provisions outlined in the University's Intellectual Property Policy. In cases where information or materials qualify as intellectual property under that policy, such as faculty-created course materials, student works, or inventions, the ownership and usage rights shall be governed by the Intellectual Property Policy. All users (employees, contractors, vendors, or others) of Information Systems are responsible for adhering to both this policy and the Intellectual Property Policy.

Policy statement

Definitions

- *Agent*, for the purpose of this policy, is defined as any third-party that has been contracted by the University to provide a set of services and who stores, processes or transmits Institutional Data as part of those services.
- *Chief Information Security Officer*, is defined as the highest ranking ITS employee or third-party security partner contracted by Nebraska Wesleyan University.
- *Information System*, is defined as any electronic system that stores, processes, or transmits information.
- *Institutional Data*, is defined as any data that is owned* or licensed by the University.

*Subject to the exceptions noted in the Intellectual Property Policy, any work created during one's duties as an employee (including a student employee) who is not a faculty member will be considered a Work-for-Hire and solely owned by Nebraska Wesleyan University.

Security Policy

Throughout its lifecycle, all Institutional Data shall be protected in a manner that is considered reasonable and appropriate, as defined in documentation approved and maintained by the Office of the Chief Information Security Officer, given the level of sensitivity, value, and criticality that the Institutional Data has to the University.

Any Information System that stores, processes or transmits Institutional Data shall be secured in a manner that is considered reasonable and appropriate, as defined in documentation approved and maintained by the Office of the Chief Information Security Officer, given the level of sensitivity, value and criticality that the Institutional Data has to the University.
Individuals who are authorized to access Institutional Data shall adhere to the appropriate Roles and Responsibilities, as defined in documentation approved and maintained by the Office of the Chief Information Security Officer.

Exceptions
The University recognizes that there may be academic or research pursuits that require deviations from these policies, standards, and procedures. Therefore, the University has developed an exception process that users may utilize to justify such deviations and document the associated risks. Exceptions to any portion of this policy require an acceptance of risk and must be jointly approved by the appropriate level of authorization outlined in ITS-01: Policy Exception Standard Process. Approvers for policy exceptions include the President, Provost or Vice President and CIO. Exceptions that have been reviewed and accepted will be documented and maintained by ITS and Risk Management.

Application and Enforcement
This Policy applies to all employees and students of the University. Failure to comply with University IT policies may result in sanctions related to an individual's use of IT resources.
Inappropriate behavior in the use of computers will be addressed through university policies and related procedures regarding students, faculty, and staff. The offenses mentioned in this policy range from relatively minor to extremely serious, though even a minor offense may lead to more significant consequences if it is repeated or malicious. Certain offenses may also be subject to prosecution under federal, state, or local laws.

The University considers the intent, severity, and history of any incident when determining an appropriate response. Sanctions for offenses will utilize procedures outlined in the Student Code of Conduct, Human Resources policies, or the Faculty Handbook.

Restrictions of Privileges During Investigations
During the course of an investigation of alleged inappropriate or unauthorized use, and after assessing the possible risk to the university or its computing resources, it may be necessary to temporarily suspend a user's network or computing privileges. This is a precautionary measure and does not imply wrongdoing by the individual involved. For example, if a computer account has been used to launch an attack on another system, that account will be rendered inactive until the investigation is complete. This is a necessary action taken to prevent further misuse and does not presume that the account holder initiated the misuse.

Unsubstantiated reports of abuse will not result in the suspension of accounts or network access unless sufficient evidence is provided to show that inappropriate activity occurred. For example, if someone reports that their computer was "attacked" by a Nebraska Wesleyan system, the burden will be upon the complainant to provide sufficient data logs or other evidence to show that the incident did, indeed at least appear to be an attack.

Review and Update
This Policy shall be reviewed and amended by the University's Chief Information Officer at increments no longer than every three (3) years or may be updated periodically for accuracy and clarity based on changes in technology or regulatory requirements.

The NWU Administrative Council approved this policy to be implemented on July 1, 2025. All topics or questions addressed in this policy that occur on or after this date will be subject to this policy and corresponding procedures. This policy supersedes and takes precedence over any prior IT policy or related procedures.

Last revised date July 1, 2025