# Executive Memorandum No. 16

## Policy for Responsible Use of University Computers and Information Systems

### 1. Purpose

It is the purpose of this Executive Memorandum to set forth the University of Nebraska guidance relating to responsible use of the

electronic devices, software, and information systems within the academic and employment setting of the University. This Policy supersedes and takes precedence over any conflicting, contradictory, or inconsistent campus, college, school, department, or faculty policies, statements, guidelines, or guidance.

### 2. General

The University strives to maintain access to local, national, and international sources of information for its faculty, staff, students, administrators, Regents, and others with tmosphere that encourages sharing of

educational, research, and public service missions. Access to and use of electronic Information Systems and University devices at the University is not a right but is a benefit of employment which may be removed at the sole discretion of the University in the event of misuse or violation of this Policy. All users must act honestly and responsibly. Every user is responsible for the integrity of these information resources. All users must respect the rights of other computer users, respect the integrity of the physical facilities and controls, and comply with all pertinent license and contractual agreements related to University Information Systems. All users shall act in accordance with these responsibilities, and the relevant local, state, and federal laws and regulations.

The University is a provider of a means to access the vast and growing amount of information available through electronic information resources. The University is not a regulator of the content of that information and takes no responsibility for the content of information, except for that information the University itself and those acting on its behalf create. Any person accessing information through the University Information Systems must determine for themselves and their charges whether any source is appropriate for viewing.

an agreement on behalf of the user or other individual accessing such Information Systems to abide and be bound by the provisions of this Policy. The University may restrict or prohibit the use of its Information Systems in response to complaints presenting evidence of violations of University policies or state or federal laws. When it has been determined that there has been a violation, the University may restrict or prohibit access by an offending party to its Information Systems through University-owned or other computers, remove or limit access to material posted on University-owned computers or networks, and, if warranted, institute other disciplinary action.

## 3. Definitions

privacy of all individuals for whom the University maintains records; and refrain from invading the privacy of individuals or entities that are creators or authors of information resources. The University employs numerous measures to protect the security of its IT resources and user accounts. Users should be aware, however, that no Information System is completely secure. Persons both within and outside the University may find ways to access files. Accordingly, the University cannot electronic information resources.  Moreover, the University does not guarantee the confidentiality or security of data, email, or other information transmitted or stored on University electronic information resources.  When University officials believe a user may be using electronic information resources in a way that may violate University policies or federal, state, or local law, or the user is engaged in

The University and its campuses may maintain accounts on external services hosting social, informational, and other content. In general, these accounts are the property of the University, administrative unit, or the department or unit that maintains them. All content provided through these accounts shall be in compliance with University policies.

## 10. University Networks and Systems for University Business

Enterprise-wide University Systems and Networks, such as but not limited to learning management, email, storage, identity and security services, shall be used for University Business and University data and records (institutional and research) shall not be stored outside of University Information Systems. University Systems and Networks have appropriate security safeguards in place to protect University data and records and are management services in accordance with ITS-06: Configuration Management Standard.

b. All University-owned Endpoints and Systems must enable access control measures such as a password or biometric controls which comply with ITS-02: Access, Identification, and Authorization Standard.

c. Endpoint device management, inventory software, and antivirus/antimalware software are provided by the Office of the Vice President for Information Technology or the IT organization that supports UNMC and are required to be installed and kept up to date on all University-owned Endpoints and Systems.

d. Endpoints and Systems where it is not technically feasible to leverage enterprise-wide endpoint management services shall follow Executive Memorandum No. 42, Minimum Security Controls, and ITS-06: Configuration Management Standard.

University Networks will be managed by the Office of the Vice President for Information Technology or the IT organization that supports UNMC.

## 13. Vulnerability Management

All University Information Systems procured or developed with University resources will be subject to inventory, scanning, and security review in accordance with ITS-13: Risk Management Standard. All scanning and security reviews will be conducted under the supervision of the Office of the Vice President for Information Technology or the IT organization that supports UNMC. Information Systems are required to meet ITS-06: Configuration Management Standard to be allowed to access the network.

## 14. Operating System and Application Patch Management

All operating systems and applications must be patched and updated in accordance with ITS-17: System and Informational Integrity Standard.

## 15. Removable Media/Media Protection

Removable media is intended to facilitate the transfer of data between Information Systems and not intended for storage or long-term archive in accordance with ITS-09: Media and Protection Standard. University data and records shall be stored on University Information Systems as defined in Section 10 of this Policy. Removable media can be used to transfer high or medium risk data only if the media or data is encrypted in a manner consistent with the data requirements. Removable media storing University data

## 16. Password Management

Authenticators and authentication strength shall meet or exceed a level of assurance which aligns with Executive Memorandum No. 42 (Policy on Risk Classification and Minimum Security Standards):

a. Services that provide access to High Risk Data shall be protected by NIST 800-63-3 Authenticator Assurance Level 2 (AAL 2).

b. Services that provide access to Medium Risk Data shall be protected by NIST 800-63-3 Authenticator Assurance Level 1 (AAL 1).

Two-Factor Authentication (AAL 2), which requires proof of possession and control of two distinct authentication factors, should be used wherever possible.

## 17. BYOD Devices

University employees, agents, affiliates, or workforce members who use personally owned devices for University-related business are responsible for maintaining device security, data return and deletion, incident reporting, response to public records requests and discovery requests, and must produce their devices for inspection when required as indicated in ITS-19: Security of Personally Owned Devices.

Only when necessary, for the performance of University-related duties and activities, and after approval of a policy exception, shall high risk data be accessed, transmitted, processed, or stored on personally owned devices, non-University owned cloud services, network attached storage, or removable storage devices (USB drives, memory cards, or similar portable drives and devices). University employees, agents, affiliates, or workforce members shall take all required, reasonable, and prudent actions necessary to ensure the security and retention of high risk data on personally owned devices. Units shall request on an individual basis whether to allow University employees, agents, affiliates, or workforce members to use personally owned devices to access or maintain high risk data. The process to request an exception is defined in Section 18 of this Policy.

## 18. Exception Process

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 a college/division leader and the Office of the Vice President for Information Technology through an exception process that has been reviewed and accepted by Risk Management. The process and procedure for exceptions is defined in ITS-01: Policy Exception Standard.

## 19. Review and Update

This Policy shall be jointly reviewed and amended by the Office of the Vice President for Information Technology and the Office of the Vice President and General Counsel at increments no longer than five years.

## 20. Application and enforcement

This Policy applied to all administrative units of the University. The University of Nebraska System and each University campus is encouraged to provide supplemental policy guidance consistent with this Policy, designed to implement the provisions herein. Failure to comply with University IT policies may result in sanctions related to the onnel and student policies up to and including expulsion for students and termination of employment for employees.

Dated this 11th day of May, 2022.

/s/
Ted Carter, President

Reference: May 11, 2022
August 28, 2001