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 System ("University") Policy and provide guidance relating to responsible use of the University's devices and electronic Information Systems. The Policy contained within this Executive Memorandum serves as the University's definitive statement on the use of 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 approved access (the "users"), and to provide an atmosphere that encourages sharing of knowledge, the creative process, and collaborative efforts within the University's 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.

Accessing any account and/or using the University's Information System shall constitute 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

For purposes of this Policy the following definitions shall apply:

a. Electronic communications shall mean and include the use of Information Systems in the transmitting, receiving, storing, or posting of information or material by way of email, message boards, forums, chat, websites, institutional social media accounts, or other such electronic tools over the Internet or other networks.

b. Information Systems shall mean and include endpoints, networks, systems, services, and other similar devices that are administered, owned, or operated by the University or for which the University is responsible.

   i. Endpoints shall refer to desktops, laptops, tablets, mobile devices, printers, or any other device, excluding servers, capable of connecting to the University network or accessing University data.

   ii. Networks shall mean and include wired and wireless video, voice, and data infrastructure, including security devices.

   iii. Systems shall mean and include software, server, storage, licensed platforms, and cloud-based services.

c. University devices shall mean and include any device purchased with University funds (including but not limited to state, foundation, grant, contract, etc.) capable of connecting to University networks directly or throughout a gateway. Examples include, but are not limited to, desktops, laptops, tablets, printers, IoT devices, servers, appliances, and sensors.

d. Bring Your Own Device (BYOD) shall pertain to personally owned Endpoints used to connect to and access University Information Systems.

e. Removable Media shall mean devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. Examples can be found in the ITS Removable Media/Media Protection Standard.

f. Records and Data are defined in Executive Memorandum No. 41, Executive Memorandum No. 42, ID-01: Institutional Data Policy, and Regents' Policy 6.7 and include institutional and research data.

g. Obscene with respect to obscene material shall mean: (1) that an average person applying contemporary community standards would find the material taken as a whole predominantly appeals to the prurient interest or a shameful or morbid interest in nudity, sex, or excretion, (2) the material depicts or describes in a patently offensive way sexual conduct specifically set out in Neb. Rev. Stat. §§ 28-807 to 28-809, as amended, and (3) the material taken as a whole lacks serious literary, artistic, political, or scientific value.

4. Permitted Uses

a. University Business Use and Limited Personal Use. University Information Systems are to be used predominantly for University-related business. However, personal use is permitted so long as it conforms with this Policy and does not interfere with University operations or an employed user's performance of duties as a University employee. As with permitted personal use of telephones for local calls, limited personal use of Information Systems does not ordinarily result in additional costs to the University and may result in increased efficiencies. Personal use of any University Information System to access, download, print, store, forward, transmit, or distribute obscene material is prohibited. Under all circumstances, personal use by employees must comply with Subsection b. of this section and shall not conflict with an employee's performance of duties and responsibilities for the University. Personal use may be denied when such use requires an inordinate amount of Information Systems resources (e.g., storage capacity or network bandwidth).

b. Priority Approval Required for Personal Use for Outside Consulting, Business, or Employment. Personal use of University Information Systems resources or equipment by any user for personal financial gain or in connection with outside (non-University) consulting, business, or employment is prohibited, except as authorized for employees by Section 3.4.5 of the *Bylaws of the Board of Regents* regarding outside employment. Employee personal use in conjunction with outside professional consulting, business, or employment activities is permitted only when such use has been expressly authorized and approved by the University Administration or the Board of Regents, as appropriate, in accordance with the requirements of and as defined by Section 3.4.5 of the *Bylaws*.

5. Access

Unauthorized access to Information Systems is prohibited. No one shall use the identity of another; nor shall anyone provide their authenticators/passwords to another. As individuals' relationships with the University change or terminate, their authorized access

to systems, services, and data shall be adjusted in accordance with Board of Regents or other University policies.

6. Misuse of Computers and Network Systems

Misuse of University Information Systems is prohibited. Misuse includes, but is not limited to, the following:

a. Attempting to modify or remove Endpoint equipment, software, or peripherals without proper authorization.

b. Accessing Information Systems without proper authorization, including Information Systems associated with the University, regardless of whether the resource accessed is owned by the University or the abuse takes place from a University site.

c. Taking actions, without authorization, which interfere with the access of others to Information Systems.

d. Circumventing authentication and authorization controls.

e. Using Information Systems for any illegal or unauthorized purpose.

f. Circumventing security measures required for Information Systems to meet security standards.

g. Storing, processing, analyzing, transmitting, or receiving University records and data on Information Systems that do not meet minimum security standards for the data classification as defined in Executive Memorandum No. 42.

h. Personal use of Information Systems or electronic communications for personal financial gain or non-University consulting, business, or employment, except as expressly authorized pursuant to Section 3.4.5 of the *Bylaws of the Board of Regents*.

i. Sending any fraudulent electronic communication.

j. Violating any software license or copyright, including copying or redistributing copyrighted software, without the written authorization of the software owner.

k. Using electronic communications to violate the property rights of authors and copyright owners.

l. Using electronic communications to harass or threaten users in such a way as to create an atmosphere which unreasonably interferes with the academic or the

employment experience. Similarly, electronic communications shall not be used to harass or threaten other information recipients, in addition to University users.

m. Using electronic communications to disclose proprietary information without the explicit permission of the owner except as permitted under Executive Memoranda Nos. 22 and 43.

n. Accessing other users' Information Systems, information, or files without their express permission except as permitted in Section 7 below.

o. Academic dishonesty.

p. Forging, fraudulently altering or falsifying, or otherwise misusing University or non-University records (including computerized records, permits, identification cards, or other documents or property).

q. Using Information Systems to hoard, damage, or otherwise interfere with academic resources available electronically.

r. Using Information Systems to steal another individual's works, or otherwise misrepresent one's own work.

s. Using Information Systems to fabricate research data.

t. Launching a computer virus, malware, phishing attack, or other rogue or malicious program.

u. Downloading or posting illegal, proprietary, or damaging material to a University Endpoint.

v. Transporting illegal or damaging material or proprietary material without authorization across a University Network.

w. Personal use of any University Information System to access, download, print, store, forward, transmit, or distribute obscene material.

x. Violating any state or federal law or regulation in connection with use of any Information System.

7. Privacy

a. User Privacy Not Guaranteed. The University is committed to respecting the privacy of individuals and will safeguard information about individuals subject to limitations imposed by federal and state law and other provisions. Members of the University community should respect the privacy of other community members, regardless of whether their accounts are securely protected; respect the

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 and does not guarantee user privacy and users should be continuously aware of this fact. Moreover, while University Information Systems are not routinely monitored for content, the University retains the right to review files, emails, and data for compliance with policy and its business purposes. Use of University Information Systems constitutions acknowledgement that users have no expectation of privacy, and consent to University review.

b. Repair and Maintenance of Equipment. Users should be aware that on occasion duly authorized University information technology personnel have authority to access individual user files or data in the process of performing repair or maintenance of computer equipment the University deems is reasonably necessary, including the testing of systems in order to ensure adequate storage capacity, performance, and security for University needs. Information technology personnel performing repair or maintenance of Information Systems are prohibited by law from exceeding their authority of access for repair and maintenance purposes or from making any use of individual user files or data for any purpose other than repair or maintenance services performed by them.

c. Response to a Public Records Request, Administrative or Judicial Order, Law Enforcement Investigations and/or Subpoenas, or Requests for Discovery in the Course of Litigation. Users should be aware that the Nebraska public records statutes are very broad in their application. Certain records, such as unpublished research in progress, proprietary or trade secret information, and personal information in personnel and student records are protected from disclosure. However, most other University data and records contained in electronic form require disclosure, if a public records request is made. Users should remember this when creating any electronic information, especially email. Also, users should be aware that the University will comply with any lawful administrative or judicial order requiring the production of electronic data and records stored in the University's Information Systems and will provide information in electronic files or data stored in the University's Information Systems in response to a public records request or legitimate requests for discovery of evidence in litigation.

d. Response to Misuse of Information Systems or Violations of University Policy. Because University electronic information resources are state agency-owned and maintained, the University has a responsibility to monitor, audit, and assure the proper use of those resources. Although the University supports a climate of trust and respect, it must monitor systems for misuse. Therefore, users of the University electronic information resources should not have an expectation of privacy in data, email, or other information transmitted or stored on University

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 activities inconsistent with the user's University responsibilities, or for other good cause, and upon review by and with the concurrence of the Office of the Vice President and General Counsel, then the chief information security officer serving the University of Nebraska System or serving the relevant campus (the "CISO") or the CISO's designee may monitor the activities and inspect and record the files of such users'(s) University devices, Information Systems, and applications. If the CISO reasonably believes that an act of misuse as defined in Section 6 above is present or imminent such that the potential for damage to the system or the information stored within it, is genuine and serious (e.g., hacking, spamming, or theft), then the CISO or the CISO's designee may take such action as is necessary to protect the Information System and the information stored in it, including the denial of access to any University or non-University user, without prior review from the Office of the Vice President and General Counsel; provided however, that the CISO shall contact the Office of the Vice President and General Counsel as soon as possible to confirm that any protective actions taken were appropriate and within the parameters of this Executive Memorandum.

e. Access to Information Concerning Business Operations. Employees regularly carry out the business functions of the University using the University's Information Systems. Business records, inquires, and correspondence are often stored such that individuals may control the access to information stored within the University's Information System. Should any employee become unavailable, be incapacitated due to illness or other reasons, or refuse to provide the information necessary to carry out the employee's job responsibilities in a reasonably timely manner, then following consultation with and approval by the Office of the Vice President and General Counsel, Office of the Vice President for Information Technology, the Offices of the Chief Business Officers (or their designee), and the Offices of the Chief Academic Officers (or their designee) may authorize access to the employee's data and records in order to carry out University business operations on behalf of the unavailable or uncooperative employee.

8. Email

a. University Business. University faculty and staff must use University email accounts for University Business communication as defined in Section 10 of this Policy and in accordance with Executive Memoranda Nos. 22 and 43.

b. Email Forwarding. Email sent to a University-provided email service shall not be forwarded through any automated means to a non-University-provided email address.

c. Never assume that only the addressee will read your email. Be careful about attachments and broad publication messages. Copyright laws and license agreements also apply to email.

d. A University user may manually forward selected email to a non-University-provided email address when such forwarding:

i. Will not result in an inappropriate disclosure of Medium-risk or High-risk data, as defined in Executive Memorandum No. 42;

ii. Does not also automatically delete the email from the University-provided email system; and

iii. Complies with all other requirements of this Executive Memorandum.

e. Email Retention. Email messages should be deleted once the information contained in them is no longer useful or required to be retained by records retention schedules. Email messages stored in one or more backup files for business continuity (e.g., inadvertent or mistaken deletions or system failures) shall be retained for a period of time not to exceed seven days.

9. Websites, Apps, and Digital Content

The University of Nebraska System and each University campus have established standards for websites and pages published from the official internet domains of each entity (nebraska.edu, unl.edu, unmc.edu, unomaha.edu, and unk.edu). Similarly, mobile and web apps developed for and representing the institution, must also comply with these standards. These are considered to be "official" publications of the University. All official websites, apps, and other digital properties owned by the University shall prominently display the administrative unit's logo to identify it as an official University digital property. No other digital properties shall be allowed to use University logos without the express written permission of the University.

Publishers of any website, app, or digital content developed on behalf of the University shall comply with University policies and all federal, state, and local laws and regulations, including copyright laws, accessibility laws, obscenity laws, laws relating to libel, slander, and defamation, and laws relating to piracy of software. Further, publishers must comply with privacy and security policies, and any other relevant policies as defined by the University or its campuses.

Publishers are responsible for the accuracy of content. Content should be reviewed on a timely basis to assure continued accuracy. All websites and apps must include a means by which users may provide feedback to the content publishers.

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 managed and administered by University Information Technology employees. Contracts associated with and for University Systems and Networks contain provisions that require appropriate technical safeguards and security measures to protect the confidentiality of University records and data and address responsibilities in the event of a data breach.

When Systems and Networks are offered universally across the University of Nebraska System by the Office of the Vice President for Information Technology, duplicative Systems and Networks shall not be provided by other divisions of the University without an approved exception.

The Office of the Vice President for Information Technology may be delayed, unable to diagnose, or otherwise unable to provide support in the event of problems with data or records stored in a non-University approved System or Network, significantly increasing the risk associated with privacy, data loss, and information security.

11. Security Awareness and Training

All University users accessing University Information Systems will participate in the University's security awareness training within thirty (30) days of commencing their employment or affiliation with a University location and annually thereafter according to ITS-05: Security Awareness Training Standards.

12. Information Systems Security

The University's Office of the Vice President for Information Technology or the IT organization that supports UNMC, provides enterprise-wide endpoint management services that shall be used to securely manage University Endpoints and Systems to comply with Executive Memorandum No. 42, Minimum Security Controls, and ITS-05: Configuration Management Standard. Requests for Endpoints and Systems to not be managed by the provided endpoint management services will be required to submit an exception process in accordance with ITS-01: Policy Exception Standard.

a. All University-owned Endpoints and Systems are to be inventoried and managed by ITS or the associated distributed IT staff leveraging enterprise-wide endpoint

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 of any classification are subject to the University data retention policies, procedures, and practices. If removable media is involved in a University e-discovery investigation, the data will be retained, and personnel must ensure that the data destruction process does not destroy any relevant 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 individual's use of IT resources or other appropriate sanctions via University personnel 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