NIAGARA UNIVERSITY	Acceptable Use of Electronic Resources	Date: 2/2021	No.
		Replaces: P-26	

PURPOSE:

Niagara University is a not-for-profit university, and its facilities, including *computer and data resources*, are to be used in furtherance of its not-for-profit, educational, research, and service purposes. More and more university activities are conducted using computers and electronic communications, with increased convenience and accessibility from and to all parts of the world. At the same time, today's inter-connected environment intensifies the risks and threats of unauthorized access to computers, inadvertent disclosures of *sensitive data*, and unexpected destruction of essential information, resulting in potentially serious consequences to individuals and to the institution. *Members of the University community* and *affiliates* interact with a wide spectrum of *sensitive data* for numerous reasons. Evolving federal and state/provincial regulations require organizations and individuals to safeguard sensitive data. With computing so widely distributed throughout NU, the responsibility to safeguard computers and data resources extends to all *members of the University community* and *affiliates*.

SCOPE:

This policy, and all policies referenced herein, apply to all members of the University community including faculty, students, administrative officials, staff, alumni, authorized guests, delegates, and independent contractors (the "User(s)" or "you") who use, access, or otherwise employ, locally or remotely, the University's Electronic Resources, whether individually controlled, shared, stand-alone, or networked/cloud based.

Definitions

1. *Affiliates* refers to individuals who have contractual or other relationships with the University and who are not employees, faculty, or students.
2. *Authorization* in this context means to grant permission to an identified individual to use a *computer or data resource*. Acceptance of *authorization* to use NU *computer and data resources* establishes an obligation on the part of the individual to use those resources responsibly.
3. *Computer and data resources* include computers and computing devices, both wired and wireless; computing, application, and database access (including passwords); software, hardware, computer, and email services; and associated computing accounts. Computers and computing devices include, but are not limited to, desktops or laptop computers, smartphones and cell phones, USB flash memory drives, or similar devices, and all other mobile devices on which High Risk Data may be sent, transmitted, viewed, received or stored.

4. *Members of the University community* refers to full- and part-time employees, faculty, and students.
5. *Sensitive data* include, but are not limited to, information about prospective, current, and former students, patients and clients of medical facilities and services, and users of legal and other services, employees and donors; also information concerning research and University business, finance and operations, and passwords. Federal and state laws and regulations, as well as University policies and office procedures, regulate the handling and reporting of many different kinds of *sensitive data*. Refer to the University's *Risk Classification Policy*. International, federal and state laws and regulations, as well as University policies and office procedures, regulate the handling and reporting of many different kinds of data. Check with the NU IT Department if you are unsure of the classification of particular data.

POLICY:

Niagara University expects *members of the University community* and *affiliates* to employ reasonable and appropriate administrative, technical, and physical safeguards to protect the *computer and data resources* that they utilize and the *sensitive data* stored on these resources. Access to *computer and data resources* (including software, hardware, computer, and email services) are privileges extended to *members of the University community* and *affiliates*, and must be exercised in conformity with all applicable NU policies and procedures and all applicable federal and state laws. Access to NU *computer and data resources* is limited to authorized personnel and is for approved purposes only. *Authorization* to use these resources is granted by Human Resources and the IT department and is pending the individual's position at the University, governed in accordance with the Hiring and Termination Guidelines. Acceptance of *authorization* to use NU *computer and data resources* establishes an obligation on the part of the individual to use these resources responsibly as defined in the Policy Requirements and Specifications below.

This policy does not form a contract of any kind, including, among others, an employment contract. The University reserves the right to modify this policy without notice and at its discretion. The current version of this policy is posted on the NU IT website (www.niagara.edu/it/policies). All terms noted in *italics* are defined at the beginning of this policy.

A. Acceptance of *authorization* to use NU *computer and data resources* establishes an obligation to:

1. behave in accordance with NU's educational, research, and service purposes and in a manner compliant with this and other applicable NU policies and procedures and all applicable laws and regulations;
2. not use your account for any commercial purposes other than those related to university business;
3. behave with civil regard for other members of the NU community and of the wider community on the Internet;
4. take reasonable steps to ensure that any computer used to access NU resources, whether it is located on an NU campus or elsewhere, is secure, virus-free, and otherwise not compromised;
5. protect the confidentiality, security, integrity, and recoverability of all *computer and data resources* and take reasonable and appropriate steps to guard these resources from improper or unauthorized use, including such use by third parties;

6. use applications that conform to NU's privacy and security policies and guidelines;
7. refrain from activities that interfere with the ability of others to use *computer and data resources*; and
8. be aware of and comply with other relevant school and University policies, procedures, and business rules and applicable local laws and regulations; in all cases the more stringent standard should be followed.

B. This obligation applies regardless of:

    1. where the computer used to access *computer and data resources* is located in an NU office, classroom, public space, or lab, or at home or elsewhere outside the University;
    2. who owns the device used to access or store the *sensitive data*; or
    3. the form or manner in which *sensitive data* are stored or transmitted, including, but not limited to, local file, shared file, file on removable media such as CD-ROM disk and jump drive, central database, fax, printer, copier, network, phone, email, or voice mail.

C. Access and use, or causing or allowing access and use, of *computer and data resources*, including email services, by anyone other than as permitted by NU is strictly prohibited by NU and by state and federal laws and may subject the violator to criminal and civil penalties as well as NU-initiated disciplinary proceedings.
D. Use of some NU *computer and data resources* may be governed by additional University, college, school, or departmental policies and procedures. Anyone authorized to use these resources is responsible to become familiar with and abide by such policies and procedures.
E. In order to safeguard the security and efficiency of *computer and data resources*, NU computer systems and NU networks are routinely monitored and recorded for integrity and operation of the system by authorized University software. *Computer and data resources* provided by NU are the property of NU and not the personal property of the individual.

Computer Security

<u>1. Safeguarding Computers for Individual Use including employee Owned Devices</u>

This section describes measures to safeguard computers typically used by individuals in NU-related activities and for accessing other University resources. As used in these operational specifications, "computers" include but are not limited to desktops or laptop computers, smartphones and cell phones, USB flash memory drives, or similar devices.

a. Physical Security

i. Do not give physical access to computers to unauthorized persons.
ii. Take appropriate precautions to prevent theft and damage.
iii. Where possible, position monitors to prevent casual viewing by visitors or passersby.

b. System Security

i. Install anti-virus software and keep virus definitions up to date.
ii. Install operating system and software patches and take other recommended steps to mitigate

known vulnerabilities of the computer in a timely manner.
iii. Do not download unauthorized software.
iv. Use a locking screensaver or other mechanism to prevent unauthorized use of the computer.
v. Do not leave your computer unattended without locking it or logging off.
vi. Do not install or use Peer-to-Peer file sharing software; this does not include DropBox or Google drive and other cloud storage solutions.
vii. Do not install or run software that requires a license without that license. Respect license agreements and do not infringe on the copyright of others - See University Copyright Policy.
viii. Respond promptly to notices from authorized University staff that vulnerabilities have been detected in your computer's system.
ix. Take particular care to secure your PurplePass and other access information (e.g., log-ins, passwords) on home computers from unauthorized use by others.
x. Do not install unsecured third-party applications that may deliver malware to a personal device on which you may have High Risk Data, thereby putting NU at breach risk.

c. Passwords

i. Where possible, secure all computer accounts with passwords, and use passwords to protect all file sharing.
ii. Use strong passwords. Strong passwords consist of at least eight (8) characters. They should not be dictionary words or readily guessable. They should include at least three (3) of the following four (4) characteristics in any order: upper case letters, lower case letters, numbers, and symbols.
iii. Change passwords every 90 days. Avoid reusing a password for at least several change iterations. If you have multiple accounts, avoid using the same password for those accounts.
v. Keep a well-secured copy of your passwords available for emergency access. Encrypt any computer file containing passwords. Keep any written file of passwords in a physically secure location, preferably separate from the computer or application they secure.
vi. Passwords for sensitive websites or email accounts should not be saved on the computer.
vii. Where possible, do not configure programs to automatically store passwords.
viii. Shut down web browsers, email programs, or other applications that might store passwords temporarily when they are not in use.

d. Remote Access (Virtual Private Network Services (VPN))

i. Any remote computer used to access NU resources must conform to these Specifications and may be subject to further resource-specific restrictions.
ii. If you do not maintain or control the remote computer, do not use it for access to, or transmission of, *sensitive data*. Access to non-*sensitive* data may be permissible. Check with the responsible department or a supervisor for guidance.
iii. Use remote access software and services with caution. Pay special attention to the configuration of remote access software, hardware, and services to ensure that they do not present a security risk to your computer or to NU. Consult with the NU IT (helpdesk@niagara.edu) for guidance on how to choose, set up, and operate remote access technologies.
iv. Obtain prior *authorization* from both your senior management and the NU IT (helpdesk@niagara.edu) before using a modem with a computer connected to the University network. Modems present a significant security risk because they enable unmonitored and uncontrolled remote access to NU's network and data.

2. Safeguarding Domain Computers

The section covers additional measures for safeguarding computers used by multiple individuals. All the operational specifications set forth above apply, as well as the following additional measures to safeguard such computers.

i. Secure all computer accounts with passwords.
ii. Give accounts to authorized persons only; provide individual log-ins. If you share a computer with others, take appropriate precautions to safeguard *sensitive data* that others may not be authorized to access and, where possible, create separate accounts for each person who is authorized to use the computer, setting appropriate permissions.
iii. Enforce use of strong passwords and periodic password changes as outlined in the Password Policy.
iv. Make every effort to maintain computer logs and review them on a regular basis.
v. Stay familiar with best practices for administering the particular computer and use them.

NU Information Security

Handling of *sensitive* information is dependent on its classification. Additional security measures are required for highly sensitive data. The following are general requirements:

a. Know what data are stored on your computer, the sensitivity of that data, and what policies apply.
b. Keep local data retention to a minimum. Rely on department, school, or University storage where you can.
c. Where possible, password protect or encrypt *sensitive data*.
d. Back up local data on a regular basis and keep the backup secure. Protect backups with the same level of security as the original data. Test backup recovery periodically to verify that it works.
e. If you use a computer shared with others, take appropriate precautions to safeguard *sensitive data* that others may not be *authorized* to access. Where possible, create separate accounts for each person who uses the computer, setting appropriate permissions.

2. Storing or Transmitting Sensitive Data

a. Do not redistribute *sensitive data* to others within or without the University, unless you are an authoritative source for and an authorized distributor of that data and the recipient is authorized to receive that data.
b. Do not allow *sensitive data* to be stored on computers or servers outside NU, unless such storage is authorized.
c. Whenever possible, *sensitive data* should be transferred in encrypted form, e.g., using SSL (Secure Socket Layer) or SSH (Secure Shell).
d. Remember that email typically is not a secure form of communication. Care should be taken to be certain that the recipient is authorized to receive that data and the address is accurate.
e. *Sensitive data*, including electronic protected health information (EPHI), Social Security numbers, or credit card information, should not be sent unencrypted via email. If use of email is necessary, use encryption technology to protect the transmission of *sensitive data* in email. This may include the use of VPN (Virtual Private Network), SSL, or encryption of the message itself using software such as PGP (Pretty Good Privacy).
f. Do not transmit *sensitive data* using instant messaging technology such as Slack, WhatsApp, and

Facebook Messenger, which use servers outside of NU. These services may allow *sensitive data* to be accessed by or stored by unauthorized parties.
g. Take special care when sending *sensitive data* by fax to make sure that it is clearly marked as confidential. Every effort should be made to ensure that only the intended recipient has access to the faxed information.
h. Keep fax machines, printers, and copiers used for sensitive data in secure areas. Faxes, printouts, and copies of *sensitive data* should be picked up promptly and handled appropriately.

3. Disposing of Sensitive Data

a. *Sensitive data* should be destroyed in a manner that prevents re-creation.
b. Reformat or physically destroy any removable storage media (such as floppy disks, zip disks, tapes, or compact disks (CD)) that contained *sensitive data* before disposing of them.
c. Shred printouts of *sensitive data*.
d. Ensure that *sensitive data* are removed from devices you use, including remote printers, before you dispose of or re-deploy those devices.

Related and Cross Referencing Policies

1. External Funding: Practice regarding Electronic Research Administration
2. Employee Cell Phones for Business Use
3. University Copyright Policy
4. Student-Owned Intellectual Property
5. External funding policy: Intellectual Property
6. University Intellectual Property and Rights Management Policy
7. Niagara University Non-Discrimination Policy and Grievance Procedures
8. University Policy on Non-Academic Student Grievance
9. Student Code of Conduct

Person	Action
Employee, student, or community member	Notices or suspects an employee violation and informs Officer, Supervisor, Department Head, or Dean, as appropriate; if uncertain, consults the Director of Human Resources. Notices or suspects a student violation and informs the Dean of Students. (See Student Code of Conduct) Notices or suspects a volunteer or community member violation and informs the Department Head of the unit coordinating the volunteer. (See reporting procedures as outlined in Non-discrimination and Grievance Procedures, Non-Academic Student Grievance policies and the most recent Collective Bargaining Agreement between NULTA and Niagara University.

Officer, Supervisor, Academic Dean, or Department Head	Assesses potential violation; if it would be a serious violation, a repeat violation, or potential violation of the law, alerts the Director of HR to determine if investigation is warranted. If the potential violation is minor, addresses the matter informally per Employee Discipline Policy. If the potential violation could be criminal, alerts Campus Safety and General Counsel. Resolved matter per the Employee Discipline Policy.
Dean of Students	Assesses potential violation for violation of student rules, including the Rules of Student Conduct, Student Athlete Code of Conduct, and Academic Integrity Policy. If investigation is warranted, works with IT Director (or designee) to ensure proper backup and authentication of Electronic Resource prior to access. If the potential violation could be criminal, alerts Campus Safety and General Counsel. Refers or addresses matter as warranted to Student Judicial, Athletics, Assistant Director of Financial Aid (student employees) or Academic Integrity Board.
Director of HR	After notification, confers with the functional officer or EVP to determine if investigation and access to Electronic Resource(s) is warranted. If investigation is warranted and approved by the functional officer, works with IT Director (or designee) to ensure proper backup and authentication of Electronic Resource prior to access. If there is a suspected violation of the law, immediately alerts both the Director of Campus Safety and the

General Counsel	Works with appropriate Officer, Supervisor, Department Head, or Dean to properly document and respond per the Employee Discipline Policy. (also see Standards of Employment)

IT Director	If the alleged violator is an employee, ensures proper permission from the functional officer is in place, and cooperates with HR Director or corporation officer to ensure investigation is conducted and content is backed up as necessary. If the alleged violator is a student, informs necessary personnel, and works with the Dean of Students to conduct investigation and backup as necessary. If an alleged violator is a community member, works with Campus Safety and any other necessary or affected parties to ensure the proper resolution.
Campus Safety	Will document occurrences and coordinate institutional cooperation with law enforcement as necessary.
General Counsel	Will assist with determining if there is a potential violation of the law, and facilitate employee cooperation with law enforcement as necessary.