DOMINICAN UNIVERSITY
Information Technology

General Information		
Title Acceptable Use Policy		**Category** Information Technology
Responsible Officer Chief Information Officer	**Effective Date** February 22, 2023	**Next Review:** February 22, 2026

I. Scope:

In addition to all members of the University community, this policy applies to any guests, vendors, or contractors.

II. Policy Summary:

This policy defines guidelines for the acceptable use of computing resources within Dominican University. Furthermore, this policy establishes the roles and responsibilities for each community member with regards to protecting information assets at the University.

III. Policy History:

New policy approved by the President's Cabinet on February 22, 2023.

IV. Policy:

Dominican University provides an array of technology resources to students, faculty, staff, and guests of the university community. These resources include, but are not limited to: electronic mail systems, web hosting, network storage space, and Internet connectivity as well as various physical resources such as university-owned computers, network cabling, wireless access points, computer workstations, kiosks, card swipes, printers, audio-visual equipment, telephone/FAX equipment, computer room equipment or wiring closets (collectively, "computing resources"). Computing resources are needed to, among other things, provide educational experiences, perform research and development, conduct business activities, and provide cost-effective communication. This policy is intended to encourage, rather than discourage, the use of computing resources at Dominican University by providing a framework for acceptable use. Dominican University reserves the right to amend this policy, from time to time, and to change, modify, and discontinue computing resources in its sole discretion.

Dominican University deeply values the privacy rights of all individuals using its computing resources. As a matter of usual business practice, Dominican University Information Technology does not routinely monitor individual usage of its computing resources. Nonetheless, users should be aware that all such computing resources are the property of Dominican University and that users do not acquire a right of privacy for communications transmitted or information stored on the institution's resources. As such, Dominican University Information Technology may access and monitor computing resources and any

information stored on or transmitted through those computing resources in its discretion. Further, in order to protect systems on the Dominican University network, Information Technology may, without prior notice if deemed necessary, remove compromised machines from the network, block malicious traffic from entering the network, and/or prohibit machines within Dominican's network from connecting to known malicious outside entities.

Acceptable Use

Computing resources at Dominican University are provided for legitimate educational and business purposes. Limited personal use of computing resources by students, staff, and faculty is permissible if it does not violate this policy or other University policies, or otherwise interfere with the legitimate education and business purposes of Dominican University.

Violations of Acceptable Use

All individuals utilizing Dominican University computing resources must do so in a responsible manner in accordance with standards of normal academic and professional ethics, University codes of conduct and policies, and all applicable laws and regulations. Violations of this policy include, but are not limited to:

- Illegal use:
  Using computing resources to upload, transmit, post, or store any material or data that, intentionally or unintentionally, violates any applicable local, state, national or international law, or violates the rules, policies, or procedures of the University or any University department is prohibited.

- Harmful action towards minors:
  Using computing resources to harm, or attempt to harm, any minor or group of minors is prohibited.

- Threats or harassment:
  Using computing resources to transmit material or data that causes or encourages physical or intellectual abuse, damage or destruction of property, or that causes or encourages harassment, explicit or implied is prohibited.

- Forgery or impersonation:
  Falsifying or removing identifying information on computing resources with intent to deceive or misguide is prohibited. Impersonation of other persons or groups with intent to harm is prohibited.

- Malicious content and spam:
  Use of Dominican University computing and messaging systems to transmit any material which contain malicious content, such as malware or phishing scams or any other content that may damage computer systems or collect or use personal information in an inappropriate manner is prohibited. Also prohibited is unsolicited commercial email (commonly referred to as spam). For purposes of training or security assessment, simulations of malicious acts (e.g. phishing) may be conducted by authorized University personnel or authorized parties outside the University with express University permission.

- Fraudulent activity:
  Using computing resources to transmit material or communications to promote a financial scam or wrongdoing is prohibited.

- Unauthorized access, threat assessments, or penetration attempts:
  Unauthorized access, threat assessments or penetration attempts of Dominican University computing resources, or a remote entity using Dominican University computing resources, is prohibited. Security assessments performed by authorized University personnel, authorized parties outside the University, or research conducted in a research and development environment disconnected from the University network and Internet, may be permitted with express University permission.

- Intercepting communications:
  The use of packet sniffers, password capture applications, keystroke loggers and any other tools that perform such similar behavior or any form of network wiretapping on computing resources is prohibited. The use of such tools to analyze or mitigate ongoing security violations may be permitted when conducted by authorized University personnel.

- Collection of data:
  The unauthorized collection of personal or University data from Dominican University computing resources without prior consent is prohibited by this and other University policies.

- Reselling services:
  Reselling, leasing or sharing University computing resources, including network access, electronic mail, web hosting, file storage or processing time, without expressed consent of the University, is prohibited. The hosting of web servers or other Internet services which perform commercial activity or any other utilization of Dominican resources to conduct business for personal gain is also prohibited.

- Service interruptions:
  Using computing resources to permit or promote activity which adversely affects the integrity or performance of computing resources is prohibited. Denial of service attacks, forged packet transmission and similar actions, without express permission of the University, are prohibited.

- Physical security:
  Unauthorized access to, destruction or alteration of, theft, damage or tampering of any physical computing resources, including network cabling, wireless access points, computer workstations, kiosks, card swipes, printers, audio-visual equipment, telephone/FAX equipment, computer room equipment or wiring closets is prohibited.

- Copyright and trademark infringement:
  Transmitting, uploading, or storing any material that infringes upon an existing copyright, trademark, patent, trade secret or other legal right using computing resources is prohibited.

- Transferring of Use
  Permission to use computing resources is granted to individuals and may not be transferred to other individuals. Sharing of a user ID/password assigned to an individual is expressly prohibited. Use of another user's ID or seeking to access another user's account is prohibited. Similarly, individuals may not use their user IDs to provide access to Dominican University's wireless network to other individuals.

- Interference with or transmission of wireless signals:
  Interfering with Dominican University's wireless networks is strictly prohibited. "Ad hoc" wireless functions must be disabled in any personal or University owned devices (e.g. printers, gaming consoles) without express permission of the University.

- Unapproved network services.
  Running network service software, which may disrupt Dominican University's network services is prohibited. The following are examples of prohibited services:
  - DHCP servers
  - DNS servers
  - Services which perform IP masquerading or NAT services
  - Routers and wireless access points

- Circumvention of controls:
  Circumventing security controls or exploiting vulnerabilities at Dominican University or at any other network from Dominican University equipment or network is prohibited. Gaining access by exceeding the limits of assigned authorization is likewise prohibited.

V. Procedures

In order to request exceptions to or report alleged violations of the aforementioned policy, please contact the Dominican University Support Center at supportcenter@dom.edu. Violations of this policy may include sanctions as outlined in the student code of conduct, staff handbook, or faculty handbook, including, but not limited to, suspension of access to computing resources, banning from campus, termination of employment, or expulsion from the University.

VI. Division Collaborations

N/A

VII. Contact Information

Information Technology
supportcenter@dom.edu
(708) 524-6888

VIII. Appendices