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

- 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:

- 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 consol