Acceptable Use Policy/Network Security

Category: Operations
Responsible Department: Information Services
Responsible Officer: Vice President of Information Services
Effective Date: 2/20/2025

Policy Summary

This Policy defines guidelines for acceptable use of computing resources within the university and explains violations of acceptable use. This policy is intended to promote a greater computer and network security posture for DePaul University and to specify unacceptable activities involving DePaul's computing facilities.

Scope

This policy affects the following groups of the University:

- Entire University Community

This policy applies to all members of the University Community, as well as any guests, vendors and contractors of the university.

Policy

DePaul University provides an array of Computing Resources to students, faculty, staff, and guests of the University community. These Computing 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. 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 DePaul University by providing a framework for acceptable use.

DePaul University deeply values the privacy rights of all individuals using its Computing Resources. As a matter of usual business practice, DePaul does not routinely monitor individual usage of its Computing Resources. Nonetheless, users should be aware that all Computing Resources are the

property of DePaul. As such, Information Services may access and monitor Computing Resources and any information stored on or transmitted through those Computing Resources, but only in accordance with applicable laws, for legitimate business purposes including, but not limited to, system monitoring and maintenance, complying with legal requirements, and administering this or other DePaul policies. Users who wish to maintain absolute privacy of information should transmit and store non-DePaul information on and through media other than DePaul University Computing Resources. Further, in order to protect systems on the DePaul network, Information Services 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 DePaul's network from connecting to known malicious outside entities.

Acceptable Use
Computing Resources at DePaul 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 DePaul.

Violations of Acceptable Use
Violations of this Policy include, but are not limited to:

a) 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.

b) Harmful Action Towards Minors
Using Computing Resources to harm, or attempt to harm, any minor or group of minors is prohibited.

c) 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.

d) 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.

e) Malicious Content and Spam
Use of DePaul 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).

f) Fraudulent Activity
Using Computing Resources to transmit material or communications to promote a financial scam or wrongdoing is prohibited.

g) Unauthorized Access, Threat Assessments or Penetration Attempts
Unauthorized access, threat assessments or penetration attempts of DePaul Computing Resources, or a remote entity using DePaul University Computing Resources, is prohibited. Use of University authentication systems including Multi-Factor Authentication (MFA) is required for a DePaul hosted and cloud hosted systems hosting DePaul nonpublic data. 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.

h) 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.

i) Collection of Data
The unauthorized collection of personal or University data from DePaul University Computing Resources without prior consent is prohibited by this and other University policies.

j) 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 is also prohibited.

k) 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.

l) 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.

m) 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.

n) 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 DePaul's wireless network to other individuals.

o) Interference with or Transmission of Wireless Signals
Interfering with DePaul's wireless networks or attaching a device to transmit a DePaul network is strictly prohibited.

p) Unapproved Network Services.
Running network service software, which may disrupt DePaul 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
- TOR or other anonymous network service
- Unauthorized pentesting tools or services

q) Circumvention of controls
Circumventing security controls or exploiting vulnerabilities at DePaul or at any other network from DePaul equipment or network is prohibited. Gaining access by exceeding the limits of assigned authorization is likewise prohibited.

(r) *Doxing*
It is prohibited to use DePaul Computing Resources to engage in doxing, which includes intentionally publishing another identifiable person's personally information (i) without their consent, (ii) with intent to harm or harass, (iii) with knowledge or reckless disregard that the person whose information is published would be reasonably likely to suffer death, bodily injury, or stalking, and (iv) resulting in the person whose information is published suffering significant economic injury, emotional distress, or fear of serious bodily injury or death of the person or a family or household member, and suffering a substantial life disruption.

s) Unauthorized Purchases
Circumventing purchasing processes and controls including use of Procards to purchase unauthorized computing equipment, software, cloud computing services, data storage, tools and utilities is prohibited. Work with Information Services and Purchasing to purchase business needed computing services and equipment.

Procedures

Reporting Violations of this Policy
Violations of this Policy may be reported through one's supervisor, Human Resources, by contacting the DePaul University Computer Security Response Team (CSRT) by electronic mail at abuse@depaul.edu, through the Misconduct Reporting Anonymous hotline: (877) 236-8390, or as otherwise permitted through University policy.

When reporting any violations of this Policy to CSRT, the following information should be provided:

a. The date and time of the alleged activity, including time zone.
b. Detailed descriptions of the alleged activity.
c. Detailed descriptions of the effects which were incurred due to this activity.

Where possible, the following information should be included:

a. The IP address used to commit the alleged activity.
b. Evidence of alleged activity including logs or packet traces.
c. Fully headered copies of any improper unsolicited electronic mail.

Questions regarding this policy or request for express permissions for use of network tools may be sent to security@depaul.edu.

Disciplinary Procedures
Violations of this policy may result in appropriate disciplinary measures up to and including termination or dismissal from the University. Violations of this Policy may also be a violation of law and may be referred to federal, state and/or local authorities, or otherwise addressed as appropriate.

CSRT Investigations
All reports submitted to the DePaul University Computer Security Response Team (CSRT) regarding an alleged computer security violation will be treated confidentially. Investigations conducted by CSRT may include interviews with suspects, correlation of event information, analysis of sensitive data, monitoring of computer systems and network use, and reporting to University management. Reports to third-party entities such as local, state or federal law enforcement agencies will be made only upon prior approval of University management or the Office of the General Counsel.

Divisional Collaborations

None.

Contact Information

DePaul University Computer Security Team
http://security.depaul.edu/

Appendices

None.

History/Revisions

Origination Date:
Last Amended Date: 9/4/2024
Next Review Date: