POLICY: ACCEPTABLE USE

DOCUMENT #:	POL-0001
EFFECTIVE	February 2023
REVIEWED:	August 2023
OWNER:	ISO

CONTENTS

1.0 PURPOSE

Illinois Wesleyan University (IWU)'s technology infrastructure exists to support the institution and administrative activities needed to fulfill the institution's mission. Access to these resources is a privilege that should be exercised responsibly, ethically and lawfully.

anitc2

The purpose of thiJ 0 the 0 Tw 31. Td [i tJ 0 5 0->>BDC -3(Un)23e3(-0.001 Tw 0.r 31. Td 268 Td [02(e)3.7 (

personal or recreational nature. Any use that disrupts the institution's mission is prohibited.

Following the same standards of common sense, courtesy and civility that govern the use of other

information will be physically secured when not in use and located to minimize the risk of unauthorized access.

- All faculty, staff, students, student workers, service providers, and guests will use approved workstations or devices to access the institution's data, systems, or networks. Non-institution owned workstations that store, process, transmit, or access confidential information are prohibited. Accessing, storage, or processing confidential information on home computers is prohibited.
- All institution portable workstations will be securely maintained by the user such me workers

4.5.3 IMPERSONATION

Usersmust not:

- Circumventthe user authentication or security of any information system;
- Add, remove, or modify any identifying network header information (“spoofing”) or attempt to impersonate any person by using forged headers or other identifying information;
- Create and/or use a proxy server of any kind, other than those provided by IWU, or otherwise redirect network traffic outside of normal routing with authorization; or
- Use any type of technology designed to mask, hide, or modify their identity or activities electronically.

4.5.4 NETWORKDISCOVERY

Usersmust not:

- Use a port scanning tool targeting either IWU’s network or any other external network, unless this activity is a part of the user’s normal job functions, such as a member of the Office of Information Technology, conducting a vulnerability scanrf4 484.8 Tm <0194>Tj /TT7.3 (w

4.7 HARDWARE AND SOFTWARE

IWU strictly prohibits the use of any hardware or software that is not purchased, installed, configured, tracked, and managed by the institution. Users must not

- Install, attach, connect or remove or disconnect, hardware of any kind, including wireless access points, storage devices, and peripherals, to any institution information system without the knowledge and permission of Information Technology;
- Download, install, disable, remove or uninstall software of any kind, including patches of existing software, to any institution information system without the knowledge and permission of the institution;
- Use personal flash drives, or other USB based storage media, without prior approval from their supervisor; or
- Take IWU equipment off-site without prior authorization from the supervisor..

4.8 MESSAGING

The institution provides a robust communication platform for users to fulfill its mission. Users must not:

- Automatically forward electronic messages of any kind, by using client message handling rules or any other mechanism without prior approval from Information Technology;
- [illegible] 7323.3 (i)-1.7 (e)0.i36 0ei1.7 (e)0.i36 0i1.7 (e)0.i36sm ( )Tj /TT0 1 T

- Only use approved methods for connecting to the institution (e.g. VPN).

4.9 OTHER

In addition to the other parts of this policy, users must not:

- Stream video, music, or other multimedia content unless this content is required to perform the user's normal business functions;
- Use the institution's information systems for commercial use or personal gain; or
- Use the institution's information systems to play games or provide similar

ILLINOIS WESLEYAN
UNIVERSITY

ILLINOIS WESLEYAN UNIVERSITY

Date	