IT Remote Access Policy

Effective Date: March 7, 2018

Approval: March 7, 2018

Maintenance of Policy: Information Technology

PURPOSE: This document details the University of Dayton's policy regarding off-campus access to its internal networks and non-public IT equipment and information resources.

SCOPE: This policy applies to all UD employees – faculty, staff, student workers as well as contractors, consultants, temporaries, and/or other agents – and to students requiring access to its internal networks and the non-public IT resources hosted therein from the Internet.

POLICY:

The University of Dayton hosts IT resources that are intended for public consumption and configured/hardened as appropriate for access directly from the Internet. The university's internal networks, its computer hosts and the various services not intended to be made publicly available are restricted to campus access. Remote access to these resources may be necessary on occasion to allow an employee to work remotely, a vendor to repair or upgrade a server, a student to collaborate on a project, etc. The following rules will apply:

- Any access to these resources requires authentication thru one of UD's formal VPN solutions. Given the nature of the resources on the Academic network, UDit will actively restrict the use of cloud-based, remote access tools - GoToMyPC, LogMeIn, Teamviewer, etc. - at the application level on that network.
- It is the responsibility of all employees and students with VPN privileges to ensure that unauthorized users are not allowed access to internal university networks and associated content. University usernames and passwords shall not be shared.
- End users shall ensure that all devices connecting remotely have current anti-virus software, are patched with respect to operating system and application updates and have firewalls enabled.
- Solutions that circumvent routing and security solutions shall be identified and disabled.
- All university acceptable use and security policies that apply to access from on-campus workstations also apply to users of remotely connecting workstations.

REFERENCE DOCUMENTS:

1. University of Dayton Telecommuting Policy
2. ISO 27002 2013 Sec. # 9.1.2
3. NIST Cybersecurity Framework PR.AC-3

POLICY HISTORY:

Approved in Original Form
March 7, 2018

POLICY (continued):

- As documented in UD's Electronic Use of Confidential Data policy, all reasonable efforts should be made to protect University data, keeping it on secured servers and devices wherever possible and never copied to personal equipment.