Drury University - Remote Access Policy

December 19, 2022

Overview

Periodically, certain job functions may require staff to access data and systems that are housed behind the Drury University firewall, while a staff member is physically located off-premises.

Remote access (via virtual private network, or *VPN*) should be restricted only to those staff members whose job function specifically requires it, as each VPN endpoint is a portal to student and institutional data that may be exposed to the public through negligence, loss, or theft.

Risks and Exclusions

Laptops and mobile devices that have VPN access to the Drury Network have the same amount of access to institutional and student data as locally connected devices. Therefore, the theft or loss of such a device poses additional risk of exposing highly confidential institutional data. **Only those users who *must* have such access, *should* be granted access.**

Remote / VPN access is expressly prohibited on personal, non-University owned devices.

It is up to each department to carefully review and police the hours of non-exempt staff who have VPN access, to ensure that only the legally permitted hours are worked remotely, and that abuses are not occurring. Any time spent working remotely by non-exempt staff must be approved by their supervisor and recorded as time worked on their timesheet.

Remote access cannot be used to work off premises when a staff member calls in sick, in order to keep from recording sick time on their timesheet.

Staff are individually liable and responsible for systems with VPN access in their possession and supervision.

Steps to Gain Remote Access

VPN or remote access may be granted to a staff member, with the written approval of their Executive Vice President. *(Please see Authorization Form, p. 3).*

Each staff member with VPN access will be required to sign an affidavit, attesting to their personal liability and pledging to protect institutional data, preserve student privacy, and keep safe all assets in their possession that have access to the institution's network resources. *(Please see Affidavit Form, p. 4).*

Drury University - Remote Access Authorization

November 9, 2021

I authorize _____ to have remote access to the Drury University network. They will need access to the following things to perform their job **(Please be specific with any applications, shared drives, remote desktops, etc that can not be accessed remotely without VPN – like EX, department shared drive name, remote desktops, etc. DO NOT enter job responsibilities below.)**:

_____

_____

_____

_____

_____

_____

_____
EVP Signature and Title

_____
EVP Name and Title (Printed)

_____
Date

Drury University - Remote Access Affidavit

November 9, 2021

I affirm that I have been granted remote access to the Drury University network, and will comply with the Remote Access / VPN Policy.

I affirm that I will not copy remote data from the Drury Network to my local device and that I am individually responsible for each device with remote access capability under my supervision.

I affirm to protect and keep safe institutional and student data, compliant with the processes and protections set forth by Drury University, as well as those protections stipulated through the ***Family Educational Rights and Privacy Act (FERPA)*** *and through the* ***Health Insurance Portability and Accountability Act of 1996 (HIPAA)****.*

I understand that information I access remotely is confidential and is intended only for the express use and benefit of Drury University.

Please Check Status Below (Please note: If Non-Exempt you will also need HR approval and signature):

___ Exempt ___ Non-Exempt

_____
HR Signature (if Non-Exempt)

_____
Staff Signature

_____
Staff Name (Printed)

_____
Staff ID Number

_____
Staff Username

_____
Date