UNITED STATES DISTRICT COURT
Middle District of Pennsylvania
IT Department

Remote Access Policy

Contents

Revision Log

Date	Description	Editor
Dec. 2019	Initial Policy	AL
June. 2020	Updated, signed and adopted	AL
Feb. 2021	No Update Required	AL
Feb. 2022	Changed Systems to IT	AL

Introduction

The ability to complete work tasks while away from the office is an ever-growing necessity as travel and other functions require staff to be away from office and have safe access to the judiciary's Data Communications Network (DCN).

Purpose

To define the parameters on how users will remotely access judicial resources on the judiciary's Data Communications Network (DCN) while working away from the office using court-provided equipment.

Scope

This policy applies to all PAMD staff and employees.

Roles and Responsibilities

PAMD Staff and Employees – Will abide by this policy, use judiciary Virtual Private Network (VPN) resources to remotely access the DCN, and to take all appropriate measures to safeguard judiciary IT assets as found in PAMD's Telework and IT security policies and procedures.

IT Department Staff – Will establish National Active Directory (NAD) permissions for remote access to the DCN. Training will be provided to each user on how to use the judiciary VPN software and remotely access the DCN.

Policy

PAMD will utilize VPN security protocols provided by the Administrative Offices of the U.S. Courts (AO) for all remote access connections to DCN resources. Only court provided laptops, iPhones, and iPads will be allowed to remotely access the DCN (no personal equipment). There may be instances when IT staff will be required to remotely access the DCN using personal laptops, such as for emergencies and testing. In these instances, the utmost care will be used to ensure that the personal hardware being used is fully security compliant in accordance with PAMD's security policies, procedures, and best practices (e.g., court provided VPN, Cisco AnyConnect, Pulse Secure and two factor authentication application DUO, up-to-date OS patches and antivirus software and other security suites).

User Types

Court Users - Are permitted remote access to PAMD and DCN resources upon telework approval by the Clerk of Court, the Chief Judge or Judge for chambers staff and Senior Managers for Support Offices. Employees and staff will be restricted from remotely accessing court resources using the judiciary-approved methods/protocols defined below. Access to PAMD and DCN resources will utilize JENIE credentials and the judiciary's DUO or Pulse Secure two-factor authentication VPN methods. Upon authorization, the IT Department staff will assist the user in setting up a VPN access profile.

Chambers Interns/Externs – Will not be provided remote access to the DCN because of security and repudiation concerns.

Access Methods and Protocols.

The following access methods have been approved and vetted for PAMD users to remotely connect to the PAMD's internal network and the DCN:

Court Provided iPhones, iPads and Smart Devices.

The Chief Judge, Clerk of Court, Chief Deputy Clerk and IT Department staff are authorized access to the DCN using court provided iPhones and iPads. This method will require a user to use approved VPN software, Cisco AnyConnect and or Pulse Secure application, which enforces two factor authentication controlled by judiciary remote access servers. NAD and JENIE credentials must be used to access the DCN.

Court Provided Laptops and Tablets.

Approved employees will use only court-provided laptops that have been specially configured and updated for using the judiciary VPN. No other remote access methods are allowed. Users are provided two choices of VPN software, either Pulse Secure or Cisco AnyConnect VPN protocols. Both applications enforce two factor authentications controlled by judiciary remote access servers. NAD and JENIE credentials must be used to access the DCN.

Access Requests

Clerk's Office Staff - Must have a completed (approved) PAMD's Telework Agreement prior to remotely accessing the DCN. Upon approval by the Approving Authority, the IT Department staff will setup hardware and assist with the training of users if necessary.

Chambers Staff - Must have approval from the Judge or the Chief Judge for teleworking. Completed Telework Agreements can be signed by the Chambers Staff. Upon approval, the IT Department staff will setup hardware and assist with the training of users if necessary.

Suspension or Termination of Remote Access

Separation - Remote access must be terminated immediately in the event of separation of a user from the judiciary, for any reason. This is normally accomplished through National Active Directory.

Disciplinary Action - In certain circumstances, when disciplinary action is taken, it may also be necessary to suspend or terminate remote access privileges. The Clerk or Chief Judge will be the approving authority for this type of action.

Security Violation - If it is determined that a remote access user is not maintaining adequate security safeguards, as specified in *Guide to Judiciary Policy, Volume 15, Chapter 3 § 330.60.60. http://jnet.ao.dcn/policy-guidance/guide-judiciary-policy/volume-15-information-technology/ch-3-security#330_60* , if the situation is not quickly remedied when brought to the attention of the employee, remote access privileges will be suspended or terminated by the Clerk or Chief Judge. The IT Director or IT Security Officer or designee is authorized to immediately suspend remote access until further guidance is provided by the Clerk or Chief Judge.

Policy Review

The Clerk of Court/CUE, IT Director or designee will review this plan annually or upon events that warrant an earlier review.

Exceptions

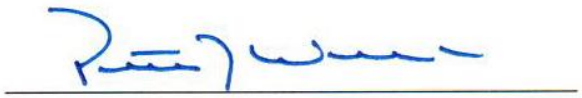
Exceptions to this policy will be documented as a component of the PAMD's Information Technology Security Exceptions Policy.

References

Guide to Judiciary Policy, Volume 15, Chapter 3 Security § 330.60.60
http://jnet.ao.dcn/policy-guidance/guide-judiciary-policy/volume-15-information-technology/ch-3-security#330_60

Policy Authorization

This policy is approved by the Clerk of Court/CUE



Date: 3-2-20