

ACCESSING WSDA'S LOCAL AREA NETWORK OR EMAIL THROUGH A REMOTE ACCESS CONNECTION

Subject Matter Lead: Chief Technology Officer

Effective Date: November 5, 2019

Accompanying Procedures: PRO-IT-603A

Accompanying Forms: [AGR-1107](#)

Cancels: POL-IT-603, dated 8/15/2008

Sunset Review Date: November 2023

Approved By: *Derek I. Sandison*

References: POL-AM-111 Protecting Privacy and Confidentiality in Public Records
POL IT-600 Internet Security
POL-IT-604 Using Electronic Messaging Systems and the Internet
[State Office of the Chief Information Officer \(OCIO\) Policy 141](#): Securing Information Technology Assets
[OCIO Policy 141.10](#): Securing Information Technology Assets Standards
[OCIO Policy 191](#): Mobile Device Usage

This policy establishes a system for requesting, approving and managing remote access to the Washington State Department of Agriculture's (WSDA's) network. Users can remotely connect to the network through Citrix, mobile.wa.gov or Outlook Web Access (OWA), and Virtual Private Networking (VPN).

Remote access provides a secure means for employees to connect from an external network to the Washington State Government Network (SGN), which includes WSDA's network.

This policy applies to all WSDA employees, represented and nonrepresented, who request or use remote access to the SGN. Represented employees refer to Collective Bargaining Agreement provisions that may supersede any portion of this policy.

1. FOR WSDA EMPLOYEES, REMOTE ACCESS MUST BE APPROVED BY THE SUPERVISOR; AND FOR THIRD PARTIES, REMOTE ACCESS MUST BE APPROVED BY THE CHIEF TECHNOLOGY OFFICER AND APPROPRIATE CONTRACT MANAGER

- In this case, the contract manager is the employee who is authorized to sign the contract with the third party.
- Supervisors determine the employee's or third party's most appropriate method of remote access based on program business need. The IT Service Desk assists supervisors in the determination process.
- Each employee must complete [AGR-1107 VPN Agreement](#), and have their supervisor sign it.

- Due to VPN's higher security risk, supervisors must annually review and update the request agreement with employees who are granted access to VPN.

2. AUTHORIZED EMPLOYEES AND THIRD PARTIES MAY ONLY REMOTELY ACCESS WSDA'S NETWORK THROUGH VPN ON WSDA-OWNED OR LEASED EQUIPMENT

3. AUTHORIZED EMPLOYEES AND THIRD PARTIES MAY CONNECT TO OWA AND CITRIX USING WSDA-OWNED OR -LEASED EQUIPMENT AND/OR PERSONAL EQUIPMENT

- WSDA'S IT staff **does not** provide support for any non-WSDA-owned or -leased equipment.

4. WORK CONDUCTED ON WSDA'S BEHALF IS SUBJECT TO THE [PUBLIC RECORDS ACT](#) AND [RECORDS PRESERVATION ACT](#)

- See *POL-IT-602 Issuing or Assigning Cell Phones and Smart Phones* and *POL-IT-604 Using Electronic Messaging Systems and the Internet*.

5. EMPLOYEES USING WIRELESS ACCESS TO WSDA NETWORKS MUST TAKE REASONABLE SECURITY MEASURES

- Privately-owned equipment will not be capable of logging in to Citrix or OWA if it does not meet IT's security standards.
- If using a personally-owned mobile device, see *POL-IT-602 Issuing or Assigning Cell Phones and Smart Phones*.
- While traveling, if the employee uses wireless service, the employee must know and adhere to usage laws and conditions. Such laws are subject to change across state and national boundaries.
- Equipment should be connected to the wireless service only for the time necessary to complete the state business activity, and be disconnected otherwise.
- Employees use current security awareness training to make informed decisions about logging into publicly available networks.

6. EMPLOYEES AND THIRD PARTY CONTRACTORS ARE RESPONSIBLE FOR PROTECTING ALL WSDA PROPERTY FROM DAMAGE, THEFT, UNAUTHORIZED ACCESS OR MISUSE BY ANOTHER PERSON

- Best practices include:
 - Keep all WSDA property in a secure location and take reasonable steps to prevent unauthorized access to the WSDA Local Area Network, Wide Area Network, email, or WSDA-supported computing environments.
 - Do not leave WSDA equipment unattended while not physically secure, no matter if it is turned on or connected to the WSDA network.
 - When traveling with WSDA equipment, employees and third party contractors should:
 - Keep equipment with them at all times, if possible.
 - Keep equipment out of sight in the vehicle when not in the vehicle.
 - Store equipment in the hotel safe when leaving it in a hotel room.
 - Keep equipment with carry-on luggage when traveling by plane, train or bus.

- Employees and third party contractors comply with the terms and conditions of all end user license agreements accompanying any hardware, software or Secure ID token (if provided VPN) distributed in connection with the remote access service.
- Employees and third party contractors are responsible for ensuring that any restricted data or confidential materials remotely accessed are appropriately used and protected in accordance with law and WSDA policies, in the same manner as if accessed from the WSDA office. This includes the required logon information for all access methods.
- Employees, third party contractors, and supervisors are responsible for making remote WSDA equipment available to IT staff on a regular basis, ideally monthly, to update anti-virus protections.
- Employees and third party contractors immediately notify the IT Service Desk if they know or suspect their network account is compromised.

7. SUPERVISORS MAY REQUEST THIRD PARTY REMOTE ACCESS, SUBJECT TO APPROVAL BY THE IT PROGRAM NETWORK CONTROL CENTER

- If approved for access, the signed contract with the third party must address VPN confidentiality before the contractor may be given access.
- To protect the WSDA network from potentially compromised equipment, third parties must use WSDA-owned or -leased equipment to connect to the SGN, whether remotely, via VPN, or on site at WSDA, unless an exception is granted by the chief technology officer.
- WSDA may terminate any third party's remote access without notice.
- WSDA equipment must be returned at the time of termination.

DEFINITIONS:

Virtual Private Network (VPN) is a network that uses a public telecommunication infrastructure, such as the internet, to provide remote offices or individual users with secure access to WSDA's network.