



# ULSTER COUNTY, NY

Department of Information Services  
25 South Manor Avenue  
Kingston, NY 12401

<b>Information Technology Policy</b>	<b>Policy No:</b> UCIS-P0325-001
<b>Remote Access Policy</b>	<b>Updated:</b> 2/9/2026
	<b>Issued By:</b> Ulster County Information Services <b>Owner:</b> Information Security Officer

## 1.0 Purpose and Benefits

The purpose of this policy is to define how all “County Entities”, as defined in Section 3.0 of this policy, will securely connect to municipal systems from remote locations.

This policy protects the confidentiality, integrity, and availability of municipal data by establishing approved remote access methods, authentication standards, and monitoring practices.

It also supports compliance with NIST CSF 2.0 on remote access.

Failure to secure and protect the Confidentiality, Integrity, and Availability of information assets in today’s highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions, and vital government functions; compromise data; and result in legal and regulatory non-compliance.

## 2.0 Authority

The Ulster County Legislature via Resolution No. 151 has approved the adoption of this policy.

Section A15-1 of the Administrative Code provides that the Director of Information Services shall have the charge and duty of performing the following functions as the County Executive may direct, including:

1. Oversee and supervise the processing of information and data within County government.
2. Develop programs designed to provide accurate, sufficient, and timely information for decision-making by all units of County government.
3. Coordinate the organization, maintenance and use of equipment capable of providing information relating to the functions of County government.
4. Direct the administrative activities of the department.

## 3.0 Scope

---

This policy applies to all “County Entities”, including employees, volunteers, temporary staff as well as third parties (such as other local governments/agencies, consultants, vendors, and contractors), that use or access any County IT resource for which Ulster County Information Services (UCIS) has administrative responsibility, including systems managed or hosted by third parties on behalf of the UCIS. This policy applies to users of any system’s information or physical infrastructure regardless of its form or format, created or used to support CEs. It is the user’s responsibility to read and understand this policy and to conduct their activities in accordance with its terms

This policy covers all remote access technologies, including but not limited to:

- Virtual Private Networks (VPNs)
- Remote Desktop or Terminal Services
- Mobile devices or laptops used off-site
- Cloud-hosted management portals
- Any system allowing remote login to County resources

## 4.0 Information Statement

---

### 2.1 Policy Overview

- Remote access shall be limited, secure, and monitored. Only approved systems, devices, and users may establish connections to the municipal network.
- All connections must use encryption, authentication, and access controls to prevent unauthorized use.
- Remote access must be used for legitimate business purposes only. Personal or non-business use is prohibited.

### 2.2 Roles and Responsibilities

- **Information Security Officer (ISO)**
  - Approves remote access solutions and ensures they comply with municipal cybersecurity standards.
  - Conducts annual reviews of remote access controls and procedures.
  - Coordinates incident response in the event of a security issue related to remote connections

- **System and Network Administrators**
  - Configure and maintain VPN and authentication systems.
  - Ensure endpoint devices meet patching, antivirus, MFA and encryption standards.
  - Maintain remote access logs and monitor for unusual activity.
- **End Users**
  - Must only use County-issued or authorized devices for remote access.
  - Must protect their credentials and never share login information.
  - Must abide by [UCIS Acceptable Use of Information Technology Resources \(AUP\)](#)
  - Must report suspected security incidents or unusual activity immediately to the Ulster County Information Services.

## 2.3 Approved Remote Access Methods

- **Municipal VPN:** The County's approved VPN is the primary method for connecting to internal systems. All VPN sessions must use multifactor authentication (MFA) and AES-256 encryption.
- **Remote Desktop Access:** Allowed only through secure gateways managed by the IT Department. MFA on the RDP protocol connection is required. Direct RDP access from the internet is strictly prohibited.
- **Mobile Devices:** Only County-approved devices enrolled in Mobile Device Management (MDM) may connect remotely.
- **Cloud Portals or Applications:** Must be approved by IT and protected with MFA and encryption.

**All other remote access tools are prohibited unless explicitly authorized in writing by the Director of IT**

## 2.4 Authentication and Access Control

- Multifactor Authentication (MFA) is required for all remote access.
- User accounts must follow the principle of least privilege.
- Temporary or elevated access must be time-limited and reviewed quarterly.
- Shared or generic accounts are not permitted.
- Passwords must comply with the County's password standards and may not be reused between municipal and personal accounts.

## 2.5 Encryption and Data Protection

- Multifactor Authentication (MFA) is required for all remote access.
- User accounts must follow the principle of least privilege.
- Temporary or elevated access must be time-limited and reviewed quarterly.
- Shared or generic accounts are not permitted.
- Passwords must comply with the County's password standards and may not be reused between municipal and personal accounts.

## 2.6 Endpoint Security Requirements

All devices connecting remotely must:

- Be County-owned or approved for remote use.
- Have up-to-date security patches and endpoint protection software.
- Be protected by an active firewall.
- Must be current with published Operating System Security Updates & Application Patches.

- Undergo periodic compliance checks by the IT Department before being granted network access.

Privately owned (BYOD) systems may not be used for remote administrative access unless approved by the Director of IT.

## 2.7 Monitoring and Logging

- All remote connections shall be logged, monitored, and reviewed.
- Logs will include username, IP address, session time, and accessed systems.
- Logs will be retained for at least one year.
- The IT Department will review remote access activity monthly for anomalies or unauthorized usage.
- Any suspicious or failed login attempts will be escalated to the IT Department for review.

## 2.8 Incident Reporting

- Users who suspect that their credentials, devices, or remote access sessions have been compromised must report the issue immediately to the Information Services or Information Security Officer.
- The County's Cyber Incident Response Plan will be activated when necessary to contain and remediate the issue.

Post-incident reviews will be conducted to identify lessons learned and update this policy accordingly.

## 5.0 Compliance

---

This policy shall take effect upon publication. Compliance is required with all enterprise policies and standards. UCIS may amend its policies and standards at any time; compliance with amended policies and standards is required.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, County Entities shall request an exception through the ISO.

Any violation of this policy may subject the user to administrative action, civil penalties, and/or criminal prosecution. The CE will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

## 6.0 Definitions of Key Terms

---

Except for terms defined in this policy, all terms shall have the meanings found in <https://ulstercountyny.gov/ucis/IT-glossary-terms>.

## 7.0 Contact Information

---

Submit all inquiries and requests for future enhancements to the policy owner at:

**Information Security Office Reference:**

**Ulster County Information Services**

## 8.0 Revision History

---

This policy shall be reviewed at least once every 2 years to ensure relevancy.

Date	Description of Change	Reviewer
10/20/2025	Draft Policy Release.	ISO
2/9/2026	Links to relevant documents	Alan Macaluso

## 9.0 Related Documents

---

### Framework

[NIST Cybersecurity Framework \(CSF\) 2.0](#)

[NYS ITS IT Security Policy](#)

### Description

The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks.)

Establishes requirements for secure remote access and encryption for state and local government systems