County of Clinton
Information Technology Policy

Remote Access Policy

Adopted: **June 9, 2021**

1.0 Purpose and Benefits

The purpose of this policy is to establish authorized methods for remotely accessing the County of Clinton's (County) internal information resources and services securely by authorized County employees, consultants, service providers, and contractors (users) performing business on behalf of a County agency or department (department).

Major security concerns with remote access include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, the availability of internal resources to external hosts, potential damage to resources, and unauthorized access to information.

2.0 Authority

This policy has been created by the Clinton County Department of Information Technology, under the direction of the Director of Information Technology, and has been approved under the authority of the Clinton County Legislature.

3.0 Scope

This policy encompasses access to all systems for which the County or department has administrative responsibility, including systems managed or hosted by third parties on behalf of the County or department, from outside the County's trusted Local Area Network (LAN).

4.0 Information Statement

Remote access is allowed when there is a clear, documented business need. Access may be allowed from County-issued or personally-owned devices at the discretion of the County and in accordance with the standards below. Such access must be limited to only those systems necessary for needed functions.

4.1 Approved Methods of Remote Access

Approved methods of remote access to systems are listed in order of preference. Multiple methods may be used together, if needed, to meet the Required Controls (e.g., accessing a portal through a tunnel connection).

a. **Direct Application Access** – accessing an application directly with the application providing its own security (e.g., webmail, https).

b. **Tunneling** - a secure communication channel through which information can be transmitted between networks (e.g., Virtual Private Network (VPN)).

c. **Portals** - a server which offers access to one or more applications through a single centralized interface that provides authentication (e.g., web-based portal, virtual desktop interface (VDI), Remote Desktop Services (RDS) Gateway).

4.2 Required Controls

a. Remote access connections must only be made through managed points-of-entry reviewed by the Information Security Officer (ISO) or Chief Information Security Officer (CISO), and approved by the Director of Information Technology. The list of approved points-of-entry shall be maintained by County IT.

b. Any method of remote access must use a centrally managed authentication system for administration and user access.

c. Devices and software used for remote access may only be approved after review by the Information Security Officer (ISO)/designated security representatives. Blanket approvals may be provided based on this review.

d. The authentication token used for remote access must conform to the requirements of the appropriate authentication management level.

e. Remote access sessions must require re-authentication after 30 minutes of inactivity.

f. Remote access sessions must not last any longer than 24 hours.

g. Departments must monitor for unauthorized remote connections and other anomalous activity and take appropriate incident response action as per the Cyber Incident Response Plan.

h. Tunneling specific controls:

   (a) Multi-Factor Authentication is required to authenticate all tunnel connections.

   (b) No split tunneling is allowed.

   (c) Network controls regulating access to the remote access endpoint and between remote devices and networks are required.

   (d) When a remote access device will have access to other networked devices on the internal network, the remote device must be authenticated such that configuration of the device is compliant with applicable policies.

i. Portal specific controls:

   a) Multi-Factor Authentication is required to authenticate all portal connections. If multi-factor authentication is not supported, the portal connection must be initiated through an established, compliant, tunnel connection.

5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all County policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, departments shall request an exception through the Chief Information Security Officer's exception process.

6.0 Definitions of Key Terms

Term	Definition
Multi-Factor Authentication	An authentication method in which a user is only granted access after successfully presenting two or more pieces of evidence (or factors). Factors include: • Knowledge (something the user knows) • Possession (something the user has) • Inherence (something the user is)
Remote Access	Access to any system for which the County or department has administrative responsibility, including systems managed or hosted by third parties on behalf of the County, from outside the County's trusted Local Area Network (LAN).

7.0 Contact Information

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

Director of Information Technology
Clinton County Department of Information Technology
137 Margaret Street, Suite 202
Plattsburgh, NY 12901

8.0 Revision History

This policy shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
06/09/2021	**Initial policy adoption**	**David Randall, Director of Information Technology**

9.0 Related Documents