ULSTER COUNTY, NY

Information Services
25 South Manor Avenue
Kingston, NY 12401

Information Technology Policy	**No:** XXXXX
Acceptable Use of Information Technology Resources	**Updated:** 9/24/2024
	Issued By: Ulster County Information Services **Owner:** Information Security Officer

1.0 Purpose and Benefits

Appropriate organizational use of information and information technology ("IT") resources, and effective security of those resources, require the participation and support of the individuals using or accessing such resources. Inappropriate use exposes the County to potential risks including, but not limited to, virus attacks, compromised network systems and services, and legal issues.

2.0 Scope

This policy applies to all "County Entities" ("CE"), 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.

3.0 Information Statement

Except for any privilege or confidentiality recognized by law, users have no legitimate expectation of privacy during any use of County IT resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed, or captured in any manner including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to users. Periodic monitoring may be conducted of systems used, including but not limited to all computer files and all forms of electronic communication (including email, text messaging, instant messaging, telephones, computer systems and other electronic records). In addition to the notice provided in this policy, users may also be notified with a warning banner text at system entry points where users initially sign on about being monitored and may be reminded that unauthorized use of the County's IT resources is not permissible.

Users accessing CE applications and IT resources through personal devices must only do so with prior approval or authorization from the CE.

3.1 Acceptable Use

All uses of information and IT resources must comply with State and County policies, standards, procedures, and guidelines, as well as State and County Executive Orders, any applicable license agreements, and Federal, State, and local laws, rules, and regulations (e.g., intellectual property laws, IRS Publication 1075).

Consistent with the foregoing, the acceptable use of information and IT resources encompasses the following duties:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information;
- Protecting County information and resources from unauthorized use or disclosure;
- Protecting personal, private, sensitive, or confidential information from unauthorized use or disclosure;
- Observing authorized levels of access and utilizing only approved IT devices or services; and
- Immediately reporting suspected information security incidents or weaknesses to the appropriate manager and the applicable Information Security Officer (ISO)/designated security representative.

For additional details regarding how users must protect County information, see Exhibit A.

3.2 Unacceptable Use

Every user has a duty to properly use County resources in a manner that will mitigate

risk to the County, to include mitigating risk of data loss, unauthorized access, acceptance of unfavorable legal terms and conditions, or compromised security of County systems or County information. The following list of unacceptable uses is not intended to be exhaustive; it is provided as a general framework for activities that constitute unacceptable use. Users, however, may be exempted from one or more of these restrictions when acting within their authorized job responsibilities, after approval from CE management, in consultation with CE IT staff (e.g., storage of objectionable material in the context of a disciplinary matter).

Unacceptable use includes, but is not limited to, the following:

- Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information;
- Unauthorized use or disclosure of County information and resources;
- Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;
- Attempting to represent the CE in matters unrelated to official authorized job duties or responsibilities;
- Connecting unapproved devices to the County network or any County IT resource;
- Connecting to any wireless network while physically connected to a County wired network;
- Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with CE policies;
- Transmitting unencrypted private information, as defined by the Internet Security and Privacy Act, via email;
- Connecting to non-County supported email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval (CEs must recognize the inherent risk in using non-County supported email services as email is often used for phishing, distributing malware, or harvesting credentials);
- Using County IT resources to circulate unauthorized solicitations or advertisements for non-County purposes including religious, political, or not-for-profit entities;
- Providing unauthorized third-parties, including family and friends, access to the CE information, IT resources, or facilities;
- Using County information or IT resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);
- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using County IT resources;
- Tampering, disengaging, or otherwise circumventing County or third-party IT security controls; and

- Using County IT resources for personal purposes when such use is not incidental and necessary, is not in a limited amount and duration, and conflicts with the proper exercise of duties of the user.

3.3 Incidental and Necessary Personal Use

Incidental and necessary personal use of IT resources is permitted, provided such use:

- is limited in frequency and duration;
- does not conflict with the proper exercise of duties of the user; and
- does not impede the ability of the individual or other users to fulfill the Department's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization.

Exercising good judgment regarding incidental and necessary personal use is important. CEs may revoke or limit this privilege at any time.

3.4 Individual Accountability

Individual accountability is required when accessing all IT resources and County information. Users are responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system, logging off at the end of your work session and protecting your credentials (e.g., passwords, tokens, or similar technology) from unauthorized disclosure. Credentials must be treated as confidential information and must not be disclosed or shared.

Users must ensure their connection of County IT resources is through a known and secured network, such as through the use of a hot spot associated with a County-issued mobile device, or a County-maintained portal that requires user authentication or where the network connection requires a password that is unique to you. A coffee shop or hotel network, for example, that is available for use without these controls is vulnerable to a cyber incident.

3.5 Restrictions on Off-Site Transmission and Storage of Information

Users must not transmit restricted Departmental, non-public, personal, private, sensitive, or confidential information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct County business. Users must not store restricted CE information that is non-public, personal, private, sensitive, or confidential on a non-County issued device, or with a third-party file storage service that has not been approved for such storage by the CE.

Devices that contain CE information must be attended to at all times or physically secured and must not be checked in transportation carrier luggage systems.

3.6 User Responsibility for IT Equipment

Users are routinely assigned or given access to County IT equipment to perform their official duties. Users must maintain proper use of the equipment and protect the equipment from theft, damage, abuse, and unauthorized use. Users must never

deliberately damage or destroy the equipment or its components. This equipment belongs to the County and must be immediately returned upon request or at the time a user is separated from CE service. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the CE.

Should County IT equipment be damaged, lost, stolen, compromised, or destroyed, users are required to promptly report the incident to their supervisor and CE's County Attorney, or the appropriate designated decisionmaker. Prompt reporting here means within twenty-four (24) hours of discovery, or earlier if possible. Users should consult the CE's County Attorney, or their designee, regarding CE's legal obligations related to a lost, stolen, or destroyed device. CE has the discretion to not issue or re-issue IT equipment to users who repeatedly lose or damage such equipment.

4.0 Compliance

This policy shall take effect upon publication. Compliance is required with all UCIS 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, CEs shall request an exception through the Information Security Office.

Any violation of this policy may subject the user to disciplinary 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.

5.0 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.

6.0 Contact Information

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

Information Security Office Reference:

Ulster County Information Services
25 South Manor Avenue
Kingston, NY 12401
Telephone: (845) 334-5300
Email:
UCIS@co.ulster.ny.us

7.0 Revision History

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

Date	Description of Change	Reviewer
7/30/2024	Original Policy Release	Alan Macaluso, Information Security Officer
9/24/2024	Final language / branding and County Attorney review	Alan Macaluso, Information Security Officer

8.0 Related Documents

Exhibit A – User Controls for Protecting County Information

The following are some examples of physical controls for handling media:

- No confidential information in e-mail subject line, as subject lines are not secure

- CE Privacy disclaimer on e- mail and fax cover sheets
  - CE must include a statement that the contents are intended for the addressed recipient only and must be deleted/destroyed if received in error.
- Reproduction of data outside normal business functions requires authorization by information owner
- Retrieval when printing/faxing
  - Users need to retrieve documents immediately or in a timely manner to protect from unintentional disclosure
- Transportation handling controls for paper both inside and outside the office
  - Hand delivery by County Entity workforce or delivery via courier (e.g., FedEx, UPS, US Postal Service)
  - Use sealed envelope addressed to specific recipient
  - Where possible obtain receipt confirmation
- Situational awareness during verbal communications
  - Be aware of surroundings when having discussions about HIGH classified information
- If choosing to label paper or portable electronic storage media, use the following: "~~UC~~ CONFIDENTIALITY-HIGH", "UC CONFIDENTIALITY-MODERATE", "UC CONFIDENTIALITY-LOW". This doesn't replace existing internal labeling structures but must be included when labeling is used to facilitate the uniform application of controls when information is shared between County Entities. If document is not bound, label each page. Label front and back covers of bound documents.