County of Ulster
Department of Emergency Services
Request for Access – Fire Records and Fire Mobile

Department: _____ **FDID:** _____

Chief of Department: _____

Primary Contact (if not the Chief): _____

Contact Phone Number: _____ **E-Mail:** _____

Check which applications are needed: ☐ **Fire Records** ☐ **Fire Mobile**

Date of Equipment Install Completion: _____

Location of Installation: _____

Computers Needing Fire Records or Fire Mobile (offices/stations) where computers are located):

_____

_____

Apparatus Needing Fire Mobile (also identify at what station):

_____

_____

Internal Use ONLY:

Date Received: _____ Date Ticket Submitted: _____

Ticket Submitted By: _____ Ticket Number: _____

List of Users, Ranks and Access (check all that apply):
A signed Ulster County Technology Security Policy for EACH user must be attached.

Name: ____________________________________ **Rank:** ____________________

☐ **Admin.** ☐ **Investigator (Chief Only)** ☐ **LOSAP** ☐ **NFIRs Adv.**
☐ **NFIRs Basic** ☐ **Personnel** ☐ **Station Activity Adv.** ☐ **Equipment**
☐ **Station Activity Basic** ☐ **Training Adv.** ☐ **Training Basic**

Name: ____________________________________ **Rank:** ____________________

☐ **Admin.** ☐ **Investigator (Chief Only)** ☐ **LOSAP** ☐ **NFIRs Adv.**
☐ **NFIRs Basic** ☐ **Personnel** ☐ **Station Activity Adv.** ☐ **Equipment**
☐ **Station Activity Basic** ☐ **Training Adv.** ☐ **Training Basic**

Name: ____________________________________ **Rank:** ____________________

☐ **Admin.** ☐ **Investigator (Chief Only)** ☐ **LOSAP** ☐ **NFIRs Adv.**
☐ **NFIRs Basic** ☐ **Personnel** ☐ **Station Activity Adv.** ☐ **Equipment**
☐ **Station Activity Basic** ☐ **Training Adv.** ☐ **Training Basic**

Name: ____________________________________ **Rank:** ____________________

☐ **Admin.** ☐ **Investigator (Chief Only)** ☐ **LOSAP** ☐ **NFIRs Adv.**
☐ **NFIRs Basic** ☐ **Personnel** ☐ **Station Activity Adv.** ☐ **Equipment**
☐ **Station Activity Basic** ☐ **Training Adv.** ☐ **Training Basic**

ULSTER COUNTY
TECHNOLOGY SECURITY POLICY

Employee ID: _____ **Ticket #:** _____
NYS Training ID # (For Internal Use ONLY)

I, _____ , have received and read a copy of Ulster County's Technology Security Policy. I understand what the County considers to be acceptable use and promise to adhere by the policy. I further understand that if I have any questions, I should call Customer Support at Extension 5381.

_____ _____
Employee Signature Date

_____
Department

Ulster County Information Services
Information Technology Security Policy

For the purposes of this document, the term user refers to any employee (permanent or temporary), contractor, consultant, vendor, volunteer, student or other person who uses, maintains, manages or is otherwise given access privileges to County systems. Additionally, the phrases "IT system" and "IT resource" include all computer, telephone, and radio hardware, fax machines, software, peripherals, applications (including electronic and voice mail), networks and network connections (including to the Internet), documentation and other capabilities intended for the purpose of processing, transferring, or storing data in support of County goals.

Shared Responsibility

All users share responsibility for the security of County IT systems. Users have access to sensitive information as part of their every day job. Misuse of Internet access, electronic and voice mail systems can expose sensitive information to unauthorized use and bring discredit on the County and its users. It is critical that County IT users avoid activities that could result in loss, corruption, or unauthorized use of sensitive information.

Policy

Users must not engage in any activities when using County IT systems that will in any way discredit the County service. Users who permit loss, corruption, or unauthorized use of information may have their access privileges terminated. County employees who permit loss, corruption, or unauthorized use of sensitive information are subject to discipline up to and including termination. Temporary employees, contractors, consultants, vendors, volunteers, students or others who permit loss, corruption, or unauthorized use of sensitive information will have all access to County IT resources revoked.

IT Resources

The County provides all of the IT resources necessary to do the job. Because the County manages costs for support, upgrades, and new capabilities, and because there are laws and regulations governing the distribution of copyrighted software, the IT manager must be able to keep track of the IT resources for each department. Users can help by working with the resources that the County provides and advising the IT Director or Designee when County-provided IT resources become inadequate for the job.

Policy

Users must not install, upgrade, or move IT resources without IT management approval, so that the IT Director or Designee can keep an accurate inventory and prevent damage to equipment. IT resources should stay in one place once they are installed. Users may reposition IT resources on a desktop or work space, but they should not disconnect the resource from the network in order to move it to a different location.

Only authorized equipment is to have a permanent physical connection to County networks. IT resources that use a temporary connection, for example dial-in via Rlink, Internet and other authorized network connections, do not need to be County owned. These connections are specifically authorized for temporary access.

No software shall be installed on any County IT system without the approval of the IT Director or Designee. Any illegal or unlicensed software will be removed upon discovery.

All software developed using County IT systems, for use on County IT systems, is the property of the County. The term software includes applications, documents, databases, other information or information systems. County-developed software must not be copied or distributed.

User IDs and Passwords

Access to County IT systems is restricted to authorized persons. This restriction is controlled by assigning an identification code, or ID, to each user account and associating a password with each ID. The user ID identifies the user to County IT systems while the password authenticates the user's identity. The password associated with a user ID both prevents unauthorized use of County IT systems and protects users from mistaken identification. The combination of a valid user ID with a correct password is key to the security and integrity of County IT systems.

Policy

Each authorized user of County IT systems will be issued a unique user ID. Before an ID is issued, each user ID request must be approved by the Department Head. If possible, the issued user ID should be used on every County IT system required by the user's job function. For specialized IT systems, a different ID may be assigned, however, the number of different user ID codes assigned to a single user must be kept to a minimum.

UC Resolution # 1999248, August 19, 1999

Upon authorization of the IT Manager, there may be a limited number of shared userids and department sign-ons assigned for specific department use. These accounts are generally named to reflect the name or purpose of a particular department for which the account is intended or to provide a means of sharing information via the use of a "shared" account for a specific purpose.

For each system that the user's job function requires, the Department Head will request a logon account with an associated password. Before the account is created, the user must meet all security requirements defined by the system or resource owner. The user's manager will only request the minimum privilege level required for the user to accomplish assigned tasks.

All users should protect their password(s) from unauthorized use. Users should take the following precautions:

- Don't write passwords down on paper or keep a file containing passwords unless that paper or file is protected in a tamper-resistant container.
- Don't give passwords to unauthorized people.
- Don't give a password to anyone over the telephone or via e-mail.
- Don't let anyone watch a user enter a password into a computer.
- Don't watch someone else as they enter their password.

Passwords are Confidential and should not be shared. Users should not share their password with anyone – including managers, system administrators, or other county personnel.

Anyone asking to use another person's password should be identified and reported to the user's immediate supervisor. If at any time, a user suspects their password has been compromised in any way, they shall immediately report the possibility to their supervisor. Supervisors should report all incidents to Department-level computer or information security personnel.

All users should follow good password construction practices, such as not using family member names. Where possible, users will be asked to create and maintain their own passwords. By protecting the user accounts assigned to them, users prevent unauthorized persons from accessing information stored on County IT systems.

Acceptable Use and Content

The performance of official County business may require the handling of a variety of information. Unacceptable use and content expend valuable resources and detract from an effective working environment.

Policy

It is every user's responsibility to utilize IT resources appropriately and ensure its security. Users must not use County IT systems for purposes other than those that support official County business or as defined in this policy.

Except when in the process of conducting law enforcement activities, users must not use County IT systems to intentionally obtain or generate information containing content that may be reasonably considered offensive or disruptive. Offensive content includes, but is not limited to, sexual comments or images, racial slurs, gender offensive comments, or any comments that would offend someone on the basis of age, sexual orientation, religious or political beliefs, national origin, or disability.

Users must not use County IT systems to conduct illegal activities.

Internet Usage

The County encourages the responsible use of the Internet as a communication and information handling tool. The authority to approve Internet access and usage, and accountability for such activities, resides with each Department or Agency Head.

Policy

In a secure and responsible manner, users may employ the Internet as a tool for gathering and disseminating information. Even though users and managers practice effective security measures, users may receive unsolicited information. County IT users and Department Heads should be informed on how to recognize unsolicited information. If received, users should call the Help Desk.

Information that is available on the Internet, and if pre-authorized by IT Management, may be downloaded and temporarily stored on County IT systems. Users should not use County IT systems to permanently store Internet information. Instead, a bookmark or hyperlink may be used to refer back to the source of the information.

UC Resolution # 1999248, August 19, 1999

Voice/Electronic Mail

The County encourages the use of voice-mail and electronic mail (e-mail) as any other work tool available to users. Users should be advised that the County backs-up electronic messages which may then be recalled or recovered for County review.

Policy

All voice-mail and e-mail messages composed, sent or received using County IT systems remain the property of the County at all times. The County reserves the right to retrieve and read any messages composed, sent, or received using County IT systems. Voice mail and e-mail will not be distributed to users other than the intended recipient except at the direction of the recipient or a Department or Agency Head.

The privacy of messages cannot be guaranteed; however, voice-mail and e-mail is generally considered to be private , but is subject to censor by the County. The County automatically screens files for potentially harmful computer programs, such as computer viruses, but the County will not retrieve the contents of messages without evidence of actual or impending harm or liability to the County.

Users should report to their supervisor if they receive voice-mail or e-mail containing content that may be reasonably considered offensive or disruptive. Supervisors should make an initial assessment to determine whether the offensive mail is a security issue, a human resources issue, or both. Once an initial assessment is complete, the supervisor should seek appropriate assistance and begin an investigation. During this investigation, security personnel and administrators must maintain the confidentiality of all individuals.

Unsolicited e-mail advertisements (a.k.a. junk mail), including those that contain offensive material, should be ignored and deleted. Do not open any attachments or click on any hyperlinks in order to reply to unsolicited e-mail. Report repetitive or significant numbers of unsolicited e-mail messages to IT management.

Privacy

The information stored on County IT systems is required to perform County business. County maintained information of a personal, private, or proprietary nature will be protected from loss, corruption, and unauthorized use.

Policy

No information will be released to non-County organizations unless a written agreement is approved by the appropriate Department or Agency Head or where required by law.

Message Authentication

Users must understand that the County does not employ methods to authenticate messages. Because of this, the County cannot guarantee that the origin of a message is as indicated by the source address. Additionally, users must understand that readers of a message may not be limited to the person indicated by the destination address.

Policy

When the authenticity of a message is in doubt, contact the message originator using a different form of communications (such as the telephone).

UC Resolution # 1999248, August 19, 1999

End-User Signature/ Date