County of Morris
Policy and Procedure

Subject: Information Services Acceptable Use Policy (AUP)		No.: 5.1.01
		Page 1 of 8
Effective Date: 05-06-19	**Revised:** 04-24-19, 07-12-17, 02-11-15	**Approval:** Board of Chosen Freeholders

I. PURPOSE

The County of Morris provides access to vast information resources including the Internet to enable its employees to be well-informed and effective in the performance of their job duties. These facilities represent a considerable commitment of resources and significant cost for telecommunications, networking, software, storage, etc. This Information Technology (IT) policy is designed to help you understand the County's expectations for use of those resources and to help you use them wisely. The policy outlines the standards, responsibilities, and procedures for the proper use and care of Morris County-owned Information Systems (IS) that also include, but are not limited to, Smart Phones, and peripheral equipment. The policy also establishes the basis by which the County will safeguard the integrity of our automation systems and protect against inappropriate use that could result in system damage and adverse financial consequences and expose Morris County to risks such as virus attacks, compromise of network systems, degradation of County services, and legal issues.

II. POLICY

A. Information Ownership and Monitoring:

Users should be aware that the data they transmit or receive on County-provided IT systems (PC's, Laptops, Tablets and Smart phones) becomes and remains the property of the County of Morris. Because of the need to protect these County IT resources, software and systems are in place that have the ability to monitor and record all usage. Therefore you should have no expectation of personal privacy or confidentiality when utilizing County IT resources and systems. The network is routinely monitored for usage patterns to maintain or increase online productivity, ensure enough access is available for official business, as well as for better planning and management of the network resources.

Morris County reserves the right to monitor, record and audit any and all activity at any time to ensure policy compliance, identify potential threats and confirm that resources are being utilized productively.

Network monitoring will also be performed for the purpose of:

1. Collecting information that is requested by law enforcement agencies.
2. Identifying inappropriate use of County IT systems.
3. Ensuring conformity with State and Federal record keeping and retention codes, regulations, and statutes of limitation.
4. Protecting the County against State criminal or civil liabilities.

B. Information Privacy

Employees must not assume electronic communications are totally private. All messages created, sent, or retrieved over the Morris County network are subject to disclosure by the County, with or without advance notice to the parties in response to Open Public Records Act (OPRA) requests, litigation discovery, suspected security violations, etc.

C. Information Security and Usage Best Practices

These rules/protocols are applicable to the use of County-issued IT systems and personal (employee owned) IT systems that are used to access County IT resources and data.

1. Morris County Network log-in credentials: Access to the County network requires the use of a minimum 20 character Passphrase.

   Passphrases must meet the following requirements:
   - Minimum length 20 characters.
   - Incorporates The following optional characteristics:
     - Special characters: space !@#$%^&*_-+=':;.,
     - Numerics
     - Uppercase and lowercase letters.

Passphrases automatically expire every 2 years requiring the selection of a new Passphrase that does not match your last 10 Passphrases. You will receive an expiration warning message 14 days, five days prior and at every attempt to log in after expiration.

Creating a Passphrase:
The following is provided as instructional information and the example phrases should not be reused.

- A quote from a book or movie ("One does not simply walk into Mordor")
- A favorite lyric from a song ("You're nobody until somebody loves you")
- Random words strung together ("horse chow clown car")

Help creating passphrases can found at web-sites such as https://www.useapassphrase.com that will generate passphrases as well as estimate how long it may take a passphrase to be cracked. For example the passphrase cited above, "horse chow clown car", and is estimated to take 3,021 centuries to crack.

Password/Passphrase Managers:
The use of a Password\Passphrase manager enables users to keep a database of their various accounts and associated passwords/passphrases. These applications run on multiple systems, such as Windows, Android phones, Apple iPhones, etc. The applications utilize sophisticated security practices to protect your information and insure it is protected from compromise or theft. You will be required to establish a master password/passphrase which, essentially, is the combination to open your safe and allows access your information. Please contact the Office of Information Technology (OIT) Help Desk, 973-285-6900, to obtain additional information about password/passphrase managers.

2. Information processing best practices: Employees must use extreme caution when opening e-mail attachments received from unknown senders, which could contain various types of malicious software/malware such as but not limited to phishing scams, viruses, e-mail bombs, Trojan horse code, etc.

To minimize the threat of viruses and other Cyber Security threats from entering the Morris County network, antivirus software is loaded and activated on all IT systems. Report any suspected malicious activity to the Office of Information Technology (OIT) Help-Desk immediately 973-285-6900.

All IT systems must be approved by OIT prior to being connected to the Morris County network. Call or e-mail the OIT Help Desk (Phone 973-285-6900). The following are general guidelines and best practices that need to be followed to ensure the security of Morris County IT systems and information processed:

- Use only licensed, accredited, and OIT authorized software on County-owned IT systems. OIT must approve loading of any software in advance. See the IT web-page on MorrisNet to view the Authorized Software List.
- Report any actual or suspected computer security incidents to OIT 973-285-6900.
- Call or e-mail the OIT Help Desk with any automation or computer hardware or software inquiries or problems.
- Immediately change passwords when the security of a password is suspected of being compromised or when actual compromise has been confirmed.
- Check all magnetic media (CD, DVD, Flash Drives) for malicious software; e.g., viruses, before loading onto a County system or network.
- Do not open the cabinet, tamper with, or make unauthorized hardware adjustments or alterations to or changes in software configuration to any County computer.
- Do not transfer any County computer to any other user or location without authorization from OIT.
- Do not knowingly access sites which advocate violence against individuals, organizations or society, or advocate harassment of individuals based on race, creed, color, national origin, age, or sex.
- Do not knowingly access sites of a pornographic nature.
- Do not engage in password misuse in order to access any other County or non-County computer.
- Do not attempt to access any other County or non-County computer by unauthorized means.
- Employees with the written approval of their first line Supervisor may use County IT assets on a limited basis for personal business during non-official work hours i.e. prior to and after normal business hours and/or during lunch periods. During such personal use the employee should expect neither privacy nor confidentiality. Personal use permission is a privilege - not a right - that requires supervisory approval.

3. Strictly Prohibited Activities:
   Under no circumstances is an employee of Morris County authorized to engage in any activity that is illegal under local, State, Federal or international law while utilizing County-owned resources. The list below is by no means all-inclusive, and is meant to serve as a framework for activities, which fall into the category of unacceptable use.

   - Violation of any statutorily mandated confidentiality requirements e.g. Privacy Act and HIPPA.
   - Violations of any copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Morris County.
   - Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Morris County or the end user does not have an active license is strictly prohibited.
   - Introduction of malicious programs, Malware, into the network or County IT system (e.g., viruses, worms, Trojan horses, Malicious Code, etc.).
   - Revealing your account password to others or allowing use of your account by others. This includes family and friends when work is being done at home.
   - Using County IT assets to actively engage in procuring or transmitting material that is in violation of sexual harassment, hostile workplace and Equal Employment Opportunity (EEO) laws.
   - Making fraudulent offers of products, items, or services from any Morris County IT account.
   - Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into an IT asset or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties circumventing user authentication or security of any host, network or account.
   - Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session via any means, locally or via the Internet/Intranet/Extranet.

D. Internet Access

The County, not the user, is the owner of the Internet access provided over its network; therefore the County has complete discretion over access privileges, nature of use, and content transmitted over its system, with the primary goal of making it a productive and stable environment.

Internet access is provided by the County for official business purpose to increase production and employee effectiveness only. Any improper use of County systems is not acceptable and will not be permitted.

Internet access is considered County property. Authorized users are expressly prohibited from using County-provided Internet access for personal and/or non-County business. Unless previously authorized, personal or recreational use of the County Internet Access Provider, even after hours, is forbidden.

E. Mandatory Cyber Security Training:

All employees as a condition of employment are required to successfully complete annual on-line cyber security training. The County Office of Information Technology delivers this training online and provides department heads reports of compliant and non-compliant employees for appropriate action.

Failure to attend the training and successfully test on the course material could result in denying and/or revoking access to County information services.

III. Policy Enforcement and Violations

Department Heads and Supervisors at all levels will ensure that users of County computer equipment are cognizant of permissible and unauthorized uses of that equipment. Users must know that the inappropriate use of County IT assets may be the basis for consideration of disciplinary action that could lead to termination.

Employees failing to comply with this policy can face a range of disciplinary actions up to and including termination. Contractors, not adhering to this policy will face the loss of access to County IT resources and serious violations could result in the loss of a contract.

IV. Related Policies and Forms

- Acknowledgement form (attached).

Acknowledgement

By signing this document, I acknowledge that I have received a written copy of the Information Systems Acceptable Use Policy for the County of Morris, New Jersey. I understand that when using County of Morris information systems I will be accessing an information system (IS), including any device attached to this information system that is provided for authorized use only. I understand that a violation of this policy could lead to discipline up to and including my dismissal from employment or even criminal prosecution. If you have any questions regarding this policy or any situation not specifically addressed in this policy, see your Supervisor or the Personnel Director. This policy is subject to revision. The County of Morris will adequately post revisions, but it is the user's responsibility to ensure that his/her use of the County of Morris computing and communications resources conforms to current policy and IT usage best practices.

You consent to the following conditions:

1. The County of Morris routinely intercepts and monitors communications on information systems that connect to the County network for purposes including, but not limited to, penetration testing, network operations and security, personnel misconduct (PM), law enforcement (LE), and criminal investigations.
2. At any time, the County of Morris may inspect and seize data stored on an information system connected to the County network.
3. Communications or data stored on a County-issued information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any Morris County authorized purpose.
4. County-issued information systems include security measures (e.g., authentication and access controls) to protect the County of Morris' interests and are not for your personal benefit or privacy.
5. Notwithstanding the above, using an information system does not constitute consent with respect to personnel misconduct, law enforcement, searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and/or their assistants. Under these circumstances, such communications and work product are private and confidential, as explained below:

   º Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any Morris County actions for purposes of network administration, operation, protection, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

   º The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement and Information Security). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

   º Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards.

Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of privilege or confidentiality. Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards.

º A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards. However, in such cases Morris County is authorized to take reasonable actions to identify such communications or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

º These conditions preserve the confidentiality of the communications or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, Morris County shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, it functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

_____ _____

Employee Signature Date

_____

Employee's Printed Name

_____

Department/Division