I. Policy

The use of County information assets is permitted for authorized County government business purposes to support the goals and objectives of the Cumberland County Government departments. Accordingly, County information assets are to be used in a manner that is consistent with applicable laws and regulations, in accordance with all County Government policies, and as part of the individual's assigned duties and responsibilities.

This policy is supported by the following standards and guidelines.

II. Purpose

The purpose of this policy is to establish required behaviors and provide direction to Cumberland County Government personnel regarding their roles and responsibilities with respect to the acceptable use and security of County information assets. It is also established to protect information technology resources, secure personal information, safeguard privacy and maintain the physical safety of individuals.

This Policy includes guidelines that sets a clear direction for information security and its role in supporting County departments in their efforts to carry out their respective missions and to achieve their business goals and objectives, while effectively managing risk and ensuring the confidentiality, integrity and availability of their information and information systems.

The County of Cumberland Computer Access Rules of Behavior and Acceptable Use Policy has been derived from applicable State and federal laws; industry best practices including the National Institute of Standards and Technology (NIST) Cybersecurity Framework for Improving Critical Infrastructure; NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations; the Center for Internet Security (CIS) Top 20 Critical Security Controls; the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM); lessons learned; and other New Jersey State Government business and technology related considerations.

III. Key Terms – Definitions

(a) **Department** – The term "Department" is used to refer to any Department, Commission, Board, Body, or other instrumentality of the Cumberland County Government.

(b) **User – The term "user" refers to** any County Department full-time or part-time employee, temporary worker, volunteer, intern, contractor, and those employed by contracted entities, who are provided authorized access to County information assets.

(c) **Information Asset** – An information asset is any data, Internet access, electronic mail (Email), device, or other component of an information or communications system. Assets generally include hardware (e.g. servers, laptop and desktop computers, switches), software (e.g. commercial off the shelf and custom developed applications and support systems) and information. Assets may also be referred to as information resources or systems.

IV. Department Responsibility

(a) Department management shall ensure users are provided with security awareness training in accordance with the County of Cumberland Computer Access Rules of Behavior and Acceptable Use Policy. Users are to be made aware of the security risks associated with their roles, and understand their responsibilities, as well as applicable laws, policies, standards, and procedures related to the security of County information assets;

(b) Department managers shall be responsible for ensuring that users acknowledge in writing, or electronically, their understanding of, and agreement to abide by, the terms set forth in the County of Cumberland Computer Access Rules of Behavior and Acceptable Use Policy;

(c) The Department Head shall be responsible for identifying and verifying the need and continuing need, in the event of a change in status or job mission, for Email and/or Internet access requested by any employee in their department; and

(d) The Department Head will be responsible for reporting and disciplining any breach of the County of Cumberland Computer Access Rules of Behavior and Acceptable Use Policy.

V. User Responsibilities

The rules of behavior and requirements contained in this policy apply to all users of County information assets, regardless of the Department, role, or location:

(a) Users are responsible for the security and use of their user account and all County information assets, for which they are assigned;

(b) Unauthorized access to County information and/or systems is prohibited;

(c) Users shall immediately report lost or stolen County information assets, suspected policy violations, suspected information security incidents, and suspicious activity, in accordance with their Department's reporting procedures; and

(d) Email and Internet access are Cumberland County property. Authorized users are expressly prohibited from using County-provided Email and Internet access for personal use, or for any

non-business purpose. Personal or recreational use of County provided Email and Internet access is strictly forbidden.

Guidelines: Users may also use the following channels to report suspected policy violations, suspected information security incidents, and suspicious activity:

- Immediate supervisor;
- Department HR Representative;
- Department IT Service Desk; or
- Department Information Security Office

VI. Acceptable Use

Users shall:

(a) Protect and secure County information assets;

(b) Access sensitive information assets only to conduct official Department business and only as permitted by applicable laws, regulations, and policies;

(c) Users who store, transmit, or process County data using commercial cloud services must use services provided by or sanctioned by their respective departments rather than personally obtained cloud services;

(d) Log off or lock systems when leaving them unattended;

(e) Complete security awareness training upon hire and on an annual basis thereafter;

(f) Permit only authorized users to use Department-provided information assets;

(g) Secure sensitive information (on paper and in electronic formats) when left unattended;

(h) Keep sensitive information out of sight when visitors or other individuals without authorization to view the sensitive information are present;

(i) Sanitize or destroy electronic media and papers that contain sensitive information when no longer needed, in accordance with records management and media sanitization policies;

(j) Only use personally identifiable information for the purposes for which it was collected.

(k) Only access, transmit, store, or create any discriminatory, defamatory, offensive, disruptive or otherwise inappropriate content including, but not limited to: websites that contain sexually suggestive images or content, racial slurs, gender specific comments, or any other comments that inappropriately or unprofessionally address someone's age, race, gender, color, national origin, religion, sexual orientation, disability, or veteran status with ***prior authorization from the County CISO for legitimate business purposes***.

VII. Prohibited Use

Users shall NOT:

(a) Perform any act that is illegal or otherwise in violation of any applicable Federal or County laws, or County policies;

(b) Circumvent security safeguards or reconfigure County information assets except as authorized;

(c) Access, transmit, store, or create any discriminatory, defamatory, offensive, disruptive or otherwise inappropriate content including, but not limited to: websites that contain sexually suggestive images or content, racial slurs, gender specific comments, or any other comments that inappropriately or unprofessionally address someone's age, race, gender, color, national origin, religion, sexual orientation, disability, or veteran status;

(d) Create, send, or forward any discriminatory, defamatory, offensive, disruptive or otherwise inappropriate communications. Among those communications considered inappropriate are any communications or materials that contain sexually suggestive images or content, racial slurs, gender specific comments, or any other comments that inappropriately or unprofessionally address someone's age, race, gender, color, national origin, religion, sexual orientation, disability, or veteran status;

(e) Create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings regardless of the subject matter;

(f) Send an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work-related purpose;

(g) Use another user's account, identity, or password;

(h) Download and install unapproved software applications on County owned, managed, or leased information assets;

(i) Establish new Internet web and/or social media pages or content dealing with County business, or make modifications to existing pages or content dealing with County business without authorization;

(j) Transmit, store, process, or share sensitive County information using personal or other unauthorized Internet services including but not limited to: personal email accounts, social media accounts, chat services, file storage, file synchronization, file sharing, and other unauthorized services;

(k) Exceed authorized access to sensitive information;

(l) Share sensitive information, except as authorized;

(m) Store sensitive information on mobile devices such as laptops, smartphones, USB flash drives, or on remote systems without authorization and appropriate safeguards (e.g. access controls, encryption), as stipulated by policy;

(n) Acquire, use, reproduce, transmit, or distribute any information, software or other electronic materials (e.g. movies, music) that are subject to the Privacy Act, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, transfer or export-controlled software or data;

(o) Use County information assets to conduct or promote an employee's outside employment or business interests, including but not limited to consulting for pay, buying, selling, trading, or any secondary employment purpose;

(p) Use County information assets to conduct political activity such as lobbying elected officials and participating in partisan political activities; and

(q) Add or install personal IT resources (e.g. wireless access points, software, mobile devices, etc.) to existing County information systems without the appropriate management authorization.

VIII. No Expectation of Privacy

Information assets created, purchased, leased, or licensed by the County of Cumberland including but not limited to: software (e.g. application software, application source code, systems software), physical equipment (e.g. computers, portable devices, tablets, smartphones), communications equipment (e.g. routers, switches, firewalls), electronic media (e.g. disks, tapes), services (e.g. Internet, communications, cloud), and information (e.g. databases and data files, system documentation, network diagrams) are the property of the County of Cumberland. As such, the County has the absolute right to monitor the use of such property. Accordingly, users of County information assets shall not assume their actions or use of County information assets are private or protected.

IX. Security Monitoring

In order to protect County information assets against security threats and to ensure compliance with the County and Department-specific policies, as well as applicable contractual, regulatory, and statutory requirements, County departments have the right to implement security monitoring technologies and systems, including but not limited to: anti-virus/anti-malware software, firewalls, host and network intrusion protection and intrusion detection systems, vulnerability management systems, database and application monitoring systems, data loss prevention, and web and email content filtering systems. As permissible by law, the departments' security monitoring systems and their authorized personnel have the right to monitor, audit, review, block, and log any traffic sent or received by users of County information assets, and any network traffic emanating from or sent to department networks, systems, applications, databases or other

information assets, as well as any traffic directed at the County's information assets from external sources.

X. Incidental use of Cumberland County Information Assets

The use of County information assets for personal purposes is NOT permitted as it may expose the County to unnecessary risks, may result in additional cost to County departments, and may violate other policies, applicable laws, regulatory, or contractual requirements.

In addition:

(a) Users have no inherent right to use County information assets for personal use;

(b) Users must understand that any use of County information assets including email may not be secure, is not private, is not anonymous, and may be subject to monitoring. Users do not a have a right to, nor shall they have an expectation of, privacy while using County information assets at any time, including accessing the Internet through County-provided connectivity. To the extent that users wish that their personal activities remain private, they shall avoid making personal use of County information assets;

(c) A user's incidental personal use of County information assets does not extend to the user's family members or others regardless of where the information asset is physically located;

(d) Storage of any user's personal data, including but not limited to, personal email messages, photos, contacts, voice messages, files, or documents created as incidental use must be nominal and temporary;

(e) The County assumes no responsibility for the availability, confidentiality, integrity of any user's personal data stored, processed, or transmitted using County information systems or assets;

(f) The County has no responsibility or obligation to provide access to or make copies of a user's personal data upon the user's separation from County Government employment, whether through voluntary or involuntary termination;

(g) Employees are prohibited from using County information assets to conduct or promote an employee's outside employment or business, including but not limited to buying, selling, trading, or any secondary employment purpose; and

(h) Employees may not use County information assets to conduct political activity such as lobbying elected officials and participating in partisan political activities.

XI. Additional Rules For Security and Privileged Access Users

Individuals, including but not limited to Information Technology personnel and Information Security personnel, with privileged access to County information assets shall:

(a) Only use privileged access credentials for duties that require escalated privileges;

(b) Use a standard user account for all other activities;

(c) Advise the Department of Information Technology on matters concerning information security;

(d) Assist the Department of Information Technology in developing system security plans, risk assessments, and supporting documentation;

(e) Ensure that adequate physical and technical safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need to know basis;

(f) Verify that users have received appropriate security training before allowing access to any system;

(g) Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs; and

(h) Document and investigate known or suspected security incidents or violations and report them to an immediate supervisor.

XII. Violations

Violations of this policy may result in revocation of access to County information assets and/or disciplinary action including suspension or termination. In addition, violations may be subject to civil or criminal prosecution under Federal or County law. The County of Cumberland shall not be responsible for any abuse email or use of assets by individual employees and shall not be responsible for any adverse consequences to any individual employee as a result of personal information communicated and/or released via a County asset. Policy violations will not be tolerated.