ANNE ARUNDEL COUNTY
MARYLAND

ADMINISTRATIVE PROCEDURE

Title: **Acceptable Use of County Information Technology**
Department: **Office of Information Technology**
Effective Date: **March 31, 2024**

1. PURPOSE.

The purpose of this AdminPro is to outline the acceptable use of Anne Arundel County ("County") Office Information Technology ("OIT") software and hardware resources. These rules are in place to protect the Employee and the County. Inappropriate use exposes the County to risks including virus attacks, compromise of network systems and services, and legal issues. This AdminPro shall supersede the AdminPro entitled "Security for Information Technology Resources", dated January 15, 2003.

2. APPLICATION.

This AdminPro shall apply to all Employees who have or are responsible for an account or any form of access that supports or requires an authenticator on any system that has access to the County OIT network and any system outside the OIT network that stores any County data (e.g., third-party hosted applications).

This policy applies to any use of information, electronic and computing devices, and network resources to conduct County business or interact with internal networks and business systems, whether owned or leased by the County, the Employee, or a third-party. All Employees are responsible for exercising good judgment regarding appropriate use of information, electronic and computing devices, and network resources in accordance with this AdminPro.

3. DEFINITIONS.

A. "Computing Resources" means all County information processing resources including all County owned, licensed, or managed computing services, hardware, software, and use of the County's network via physical or wireless connection regardless of the ownership of the computer or device connected to the County's network.

B. "Employee" means any County, or its subsidiaries, permanent and temporary employee, vendor, contractor, consultant, volunteer, and any other persons with authorized access to County Computing Resources.

4. POLICY.

A. General Use and Ownership.

I. Employees shall comply with the policies and guidelines for any specific set of resources to which they have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

II. Employees shall be familiar with the OIT information security policies.

III. Employees shall access, use or share County information only to the extent it is authorized and necessary to fulfill their assigned job duties.

IV. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

V. Employees shall only use the Computing Resources, computer accounts, and computer files for which they have authorization.

VI. Employees are individually responsible for appropriate use of all Computing Resources assigned to them, including the computer, the network address or port, software and hardware.

VII. Employees shall at all times ensure the physical security of the Computing Resources they are assigned.

VIII. Employees shall promptly report the theft, loss, or unauthorized disclosure of County Computing Resources to the HelpCenter.

IX. Employees shall connect their Computing Resources to the network frequently to permit the OIT support staff to install security patches.

X. Employees shall only use software approved and installed by OIT. Software does not include browser extensions.

4.1.11. Employees shall activate and utilize the screen lock feature prior to leaving the Computing Resource unattended.

B. Identity and Access.

I. Employees shall create strong passwords that comply with the OIT Password Policy.

II. Employees shall change their password in accordance with the OIT Password Policy and if the Employee suspects their password has been compromised.

III. Employees shall make a reasonable effort to protect their passwords and to secure resources against unauthorized use or access.

IV. Employees may not use another individual's account, or attempt to capture or guess other users' passwords.

V. Employees shall not allow another person to use their user ID and password on any County Computing Resource.

VI. Employees may not leave passwords unprotected.

VII. Employees may not leave their user accounts logged in at an unattended and unlocked computer.

C. Inappropriate/Illegal Content and Software.

I. Employees shall only utilize approved web-based applications and services and abide by the County's Web-based Applications and Services Policy.

II. Employees may not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the County and/or any of its Employees.

III. Employees are prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the County's Administrative Procedure entitled "Use of Social Media".

IV. Employees may not use County Computing Resources to transmit, distribute or store material that is inappropriate, as reasonably determined by the County, or material that is illegal, defamatory, libelous, indecent, obscene, pornographic, enables online gambling or inconsistent with the generally accepted practices of the County.

D. Email.

I. Employees are responsible for checking their County email account on a regular basis.

II. Employees shall use extreme caution when opening email attachments received from unknown senders, which may contain malware.

III. Employees shall use County email encryption tools to protect sensitive County data sent outside the County's domain.

IV. Employees shall not use a third-party email provider (i.e., Hotmail, Outlook) provided by any outside Internet Service Provider (ISP) or party, to send County

information or any files emanating from within the County to external recipients. This includes any County work or data forwarded to personal email addresses for working remotely, unless explicitly approved by OIT.

V. Employees may not use Computing Resources, including email, to send nuisance messages such as chain letters, spam, and profane, obscene, threatening, libelous or harassing messages.

VI. Employees may not attempt unauthorized access to the email of other County or non-County users.

VII. County emails are subject to department defined-retention policies and automatic deletion. It is the responsibility of Employees to save all email they want to retain indefinitely.

E. Government Data.

I. Employees shall protect any sensitive materials being sent, received, stored, or processed in accordance with the level of classification assigned to it, including both electronic and paper.

II. Employees are responsible for coordinating with OIT to ensure critical data is copied or backed up.

III. Employees shall upload all local electronic documents to Google Drive to ensure they are routinely backed up. An Employee's desktop/laptop hard drive is not backed up and the Employee could have a data loss should a hardware failure occur.

IV. Employees may not attempt to access data that the Employee is not authorized to use or access.

V. Employees may not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.

VI. Employees may not knowingly introduce malicious software into the County Computing Resources.

VII. Employees may not tamper with the anti-virus software installed on County Computing Resources.

VIII. Employees may not circumvent or attempt to circumvent software or hardware security controls.

IX. Employees may not attempt to access data the Employee is not authorized to use or access.

X. Employees may not connect any unauthorized device to County Computing Resources (e.g, routers, gaming consoles, streaming devices).

F. Compliance.

I. Employees shall abide by federal, state, and local laws.

II. OIT reserves the right to audit networks and systems on a periodic basis to ensure compliance with this AdminPro.

III. All messages created, sent or retrieved over the internet and email are the property of the County and may be regarded as government information and the County reserves the right to intercept, retain, read and inspect the same if the County believes, in its sole judgment, that it is justified to do so in order to protect its government.

IV. Employees shall report all breaches of information security, actual or suspected, to the HelpCenter for investigation.

V. Employees may not execute any form of network monitoring which will intercept data not intended for the Employee's host, unless this activity is a part of the Employee's normal job duties or explicitly approved by OIT.

VI. Employees shall abide by all applicable copyright laws and licenses. The County has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements.

VII. Employees may not use, copy, or distribute copyrighted works, including but not limited to web page graphics, sound files, film clips, trademarks, software and logos, unless they have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution.

VIII. OIT reserves the right to immediately and without notice withdraw and revoke temporarily or permanently an Employee's access to any and all Computing Resources if it is found that an Employee is in breach of County policies, standards or procedures, subject to disciplinary action, in line with the County's disciplinary procedures, in addition to being required to pay any appropriate part of costs and/or damages incurred.

5. PROCEDURE.

A. Compliance Measurement.

The OIT support team will verify compliance with this AdminPro through various methods, including, but not limited to, vulnerability scans, internal and external audits, and feedback to the policy owner.

B. Exceptions.

Any exception to this AdminPro must be approved by the OIT support team in advance of purchase and/or implementation.

C. Non-Compliance.

Any account, application, and/or system that does not adhere to this AdminPro may be taken offline until such time that a formal assessment and necessary remediation can be performed at the discretion of the Chief Information Officer.

Signed this 1st day of April, 2024.

DocuSigned by:
6FBC944F324F441...
Jack Martin
Chief Information Officer

DocuSigned by:
F18F9A5AA60D47F...
Christine M. Anderson
Chief Administrative Officer

Approved as to form and legal sufficiency:

DocuSigned by:
4877267C9A7E4C0...
Gregory J. Swain
County Attorney