Addendum to Acceptable and Supportable Use of Technology

POLICY NUMBER:
ADDENDUM NUMBER: 3
ADDENDUM TITLE: CLARIFICATION OF GOVERNING ACCOUNTS, LOGINS, AND ACCESS
EFFECTIVE DATE:
REVISION DATE:
APPROVED BY:
Ordinance No.
Dated the day of 2022.
An addendum, which shall be included as part of the original policy, to Policy No. 210-1000-004, Acceptable and Supportable Use of Technology.

STATEMENT OF ADDENDUM

The Columbus Consolidated Government (CCG) establishes policies regarding the acceptable and supportable use of technology. This addendum intends to provide explicit clarification regarding governing accounts, logins, and access.

SCOPE

This addendum applies to all technologies and technology-related devices which are applicable to this policy number 210-1000-004 and titled Acceptable and Supportable Use of Technology. This includes, but is not limited to, all computers, laptops, cell phones, mobile hotspots, printers, or other technology devices purchased by Columbus Consolidated Government. This addendum outlines the governance of accounts, logins, and access.

GOVERNING ACCOUNTS, LOGINS, AND ACCESS

1) It is the sole responsibility of the Director of the Department of Information Technology to provide access and access controls to computers, computer systems, networks, technology systems, and technology devices.
2) It is the responsibility of the user to engage in at least one additional step beyond the normal single login process to access certain resources. The resources that require at least one additional step beyond the normal single login process will be determined by the Department of Information Technology. This practice includes Multifactor Authentication.
3) It is the responsibility of the user to ensure the security of their login information, including usernames, passwords, passphrases, PINS, operator I.D.s, Multifactor Authentication, or any other login type or related information.
4) Users are prohibited from sharing usernames, passwords, passphrases, P.I.N.s, operator I.D.s, Multifactor Authentication, or any other login type or related information with another person.
5) Users are prohibited from using another person(s) login information, including, but not limited to, their username, password, passphrase, P.I.N., operator I.D., Multifactor Authentication, or any other login -type or related information.
6) It is a violation of Georgia law to share passwords with another user.
7) Personnel with G.C.I.C. (Georgia Crime Information Center) access must not leave their device logged into the system unattended for any length of time. Personnel without authorized access to the G.C.I.C. System must not access the system in any way at any time for any reason.
8) Users must log off or "Lock" their device when it is unmonitored.
9) Users are responsible for ensuring that their devices are not left unattended and/or logged in. Security of a user's workspace is the responsibility of the user, their supervisor(s), and building security.
10) The Director of the Department of Information Technology reserves the right to revoke, invalidate, or remove a user's usernames, passwords, passphrases, P.I.N.s, operator I.D.s, or any other login-type or related information, access or permissions at any time for any reason to protect system integrity.