**Multi-Factor Authentication**

**Policy**

The purpose of this policy is to establish standards and requirements for the use of multi-factor authentication when accessing Summit County’s Information Technology resources as well as hardware token responsibility.

Multi-factor authentication provides an additional level of security to protected accounts, reducing the risks associated with account compromise and unauthorized access.

**Procedure**

Authentication Method:

The county has adopted the ‘hardware token’ method of multi-factor authentication. The hardware token is a device that will generate a random number that will be utilized along with a 6–8-digit pin that is created by the user. Hardware tokens are to be treated as county property. If lost, the user will be responsible for the replacement cost of $20.00. Users will receive an Acknowledgement Form at the time that their device is provided. Users will also be responsible for returning the device should they leave county employment.

One hardware token will be provided to each charter agency staff and to non-charter agency staff that require access to the county’s network.

Use:

Multi-factor authentication will be required for some applications, Windows logon, and VPN access. The Office of Information will communicate as multi-factor authentication is expanded to additional applications.

Users will be responsible for having their hardware tokens with them when in the office or if working at a remote location.

Users should contact The Office of Information Technology via the ServiceNow portal or by calling 330-643-2013 should they become locked out, forget their PIN, or if they have lost or damaged their hardware token.

Enforcement:

The Office of Information Technology will leave it to the discretion of each office holder to determine how they will enforce that staff must have their hardware tokens with them. If a user loses, damages, or forgets their hardware token, they may be unable to perform some or all of their job duties due to not being able to gain access.

Emergency Access:

The Office of Information Technology can provide emergency access in critical situations should a user be unable to use their token or if they do not have their token. Emergency access must be approved by The Office of Information Technology Leadership to ensure that it does constitute an emergency. Requests for emergency access should be submitted by a Sspervisor or above level via the ServiceNow Portal or by calling 330-643-2013.

Emergency access will require contact with the Support Desk during the process and will require access to a phone.