Treasure Valley
Community College

Code: **EGADD**
Adopted**: 06/21/22**

Multi-Factor Authentication (MFA) Policy

Purpose:

The purpose of this policy is to define when the additional security provided by multi-factor authentication will be required to access Treasure Valley Community College systems. This policy is designed to minimize the potential security exposure to TVCC from damages which may result from unauthorized use of college services. Multi-factor authentication (MFA) adds a layer of security which helps deter the use of compromised credentials.

Procedure:

Most, if not all, Electronic Information Resources owned and maintained by the College for the use of employees and students require individuals to authenticate their identity before being able to access the systems.

Scope:

This policy applies to all users who access restricted or confidential data (or the systems that contain this data) outlined in the Data Classification List maintained by the Chief Information Officer. This policy applies to both on-campus and off-campus access to College resources whether the access is through College-owned or personally owned devices. This policy applies to any system that contains confidential or restricted data or that requires an additional layer of protection as determined by the Chief Information Officer.

All users who have access to confidential and/or restricted data will be required to use Multi-Factor Authentication on their TVCC system accounts.

User Requirements:

Users will be required to enroll a device to serve as the second authentication method as part of multi-factor authentication. This second device can be an office phone, cell phone, or supported authenticator app. Multiple authentication methods can be added to a single account.

- Users will set a default sign-in method from the methods added to their account.
- Users must contact Information Technology Services to report suspicious activity or a compromised account.

Personal Cell Phone Usage:

TVCC does not require the use of a personal cell phone for multi-factor authentication. It is a user's choice if they wish to enroll a personal device as a method for multi-factor authentication.

Exceptions:

Any exceptions to this policy must be approved by the Chief Information Officer.

Compliance:

When a user is found to be in violation of this policy, access to College-owned information technology resources may be revoked and the College's disciplinary process will be followed as outlined in personnel handbooks, TVCC's Faculty Collective Bargaining Agreement, TVCC Student Rights and Responsibilities, or any other applicable policies. If the matter involves illegal action, law enforcement agencies may also become involved, as would occur for matters that do not involve information technologies or the Internet.

Definitions:

User:

Any person or entity accessing, logging into, or attempting to access or log into, a College hardware or software system; or connecting to, or attempting to connect to or traverse a College network, whether by hardware or software or both, from any location. The term "User" includes faculty, staff, students, visitors, vendors, contractors, service providers, automated software programs/agents (and their developers), and any other individuals or agents who access and use College information technology.

Multi-Factor Authentication (MFA):

MFA is an extra layer of security for TVCC accounts designed to ensure the user is the only person who can access an individual account, even if someone else may know the password.