

**IT Governance Executive Committee Meeting**

**Regular Meeting: January 18, 2017**

**Item: CSUSB Access Control Standard**

**Background**

The need to incorporate additional security mechanism to protect user credential from being used for unauthorized access has become one of the major security issues given the sophistication of “phishing” attacks. Once the authentication credential of a user has been stolen, there is little that can be done to prevent the unauthorized use of those credentials to access resources on the Internet. One technology that has proven to be successful in mitigating this risk is the use of a multi-factor authentication solution. A multi-factor authentication solution consist of several pieces of evidence that need to be presented by the user for successful authentication, such as something they know, something they have, something they are. In our case the solution will consist of something they know (password) and something they have (cell phone, crypto token, etc.)

The proposed changes in the CSUSB Access Control Standards strengthen the authentication requirement for all users who have access to protected Level 1 data, significant amounts of Level 2 data or have administrative access to critical university systems or systems containing protected data to use multi-factor authentication.

In addition CSU system wide auditors have incorporated in their audits the requirement to provide additional layers of security to prevent the use of stolen credentials to access CSU sensitive data available on the internet. Multi-factor authentication is one of the solutions that several campuses are implementing in response to this audit finding.

**Alternatives**

There are no other effective alternatives to prevent an unauthorized entity to access university resources on the internet, once the authentication credential (Coyote-ID and password) of an authorized user has been stolen or compromised.

**Recommended Action**

Implement the use of a multi-factor authentication solution for those users that have administrative access to critical systems or user who have access to protected information.

**Rationale**

The use of a multi-factor authentication solution will require the end user to verify the validity of their authentication credentials by providing additional information from a physical device on their possession, preventing anyone who has only the Coyote-ID and password to gain access to a resource. The physical device could be a phone, cell phone, a tablet or a crypto token.

**Suggested time line**

Start the implementation process as soon as the standard is approved. The implementation will consist of three phases: The expectation is to have the standard fully implemented within one (1) year.

Phase I: Identification of all campus users who have access to protected Level 1 data, significant amounts of Level 2 data or have administrative access to critical university systems or systems containing protected data.

Phase II: Provide training and support on the use of the campus multi-factor authentication solution, and incorporate requirements in appropriate business process.

Phase III: Enforcing multi-factor for identified users.