****

**IT Governance Executive Committee Meeting**

**Regular Meeting –October 18, 2017**

**Item 1. Recommendation to Activate Two-Step Authentication (DUO) to CFS users**

**ITS Strategic Plan Alignment:** Stable and Secure Infrastructure 4.4.1- Deploy secure and mobile multi-factor authentication

**Background**

The need to incorporate additional security mechanisms to protect user credentials from being used for unauthorized access has become one of the major security issues given the sophistication of “phishing” attacks and the adoption of single sign-on. Once the authentication credentials of a user have been stolen, there is little that can be done to prevent the unauthorized use of those credentials to access resources online. This vulnerability was identified by the CSU auditors as a system wide finding.

One technology that has proven to be successful in mitigating this risk is the use of a multi-factor authentication (MFA) solution. A MFA consists 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 use of a two-step 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.

The solution that has been adopted by the CSU and is being deployed on campus is provided by DUO.

**Alternatives**

Continue without implementation of multifactor authentication and rely on traditional and current methods of data protection.

**Recommended Action**

Implement a Two-Step Authentication process to campus users with access to CFS before it becomes a requirement, and prevent any possible interruption on their access to CFS.

**Rationale:**

A compromise of authentication credentials for CFS users may expose confidential information such as tax-id of vendors and consultants. In addition, it may allow for the unauthorized change of payment routing information as well as the unauthorized creation of vendors, purchase orders and invoices, any of which may result in a significant financial and legal impact to the University.

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 system wide audit finding.

 In response to this CSU system wide audit finding, multi-factor authentication (MFA), specifically two-step-authentication, will be required to access the Common Financial System (CFS). This requirement will also be incorporated in CHRS.

In light of this requirement, and since two step authentication has been deployed on campus to users with access to Level 1 data, extending the deployment will ensure access to CFS without interruption once the use of MFA for CFS is enforced by the Chancellor's Office.

**Recommended Timeline:**

The implementation will consist of three phases:

**Phase I**: Identification of all campus users who have access to CFS.

**Phase II**: Provide training and support on the use of the campus two-step authentication.

Send email communication to CFS users providing information about two-step authentication November 6, 2017

**Phase III**: Enforcing two-step authentication for identified user

Activate two-step authentication for CFS users: December 11, 2017