Dear Colleagues,

Recently we have all become keenly aware of how important it is to protect the sensitive data we collect to accomplish the academic and business missions of Fresno State. There is no doubt that technology has enhanced the effectiveness of our daily activities, demanding our diligence in safeguarding the information entrusted to us.

It is the collective responsibility of University employees, within their respective areas, to ensure the protection and confidentiality of information collected from students, staff, community members, and business partners alike, while meeting the academic and business purposes at Fresno State. The loss or theft of sensitive data can have serious consequences for the individuals affected as well as the University.

With this in mind, I would like to take a moment to remind everyone of the California State University (CSU) and Fresno State information security policies, standards and practices that govern the protection, collection, retention, and disposal of sensitive information. If your role in the University requires you to use confidential information, then the following policies are ones with which you must be intimately familiar.

CSU Information Security Policies and Standards **(Please see a detailed version here.)**

CSU Policy 8065.S02, Data Classification Standard: Defines confidential (level 1) and restricted (level 2) data and why such data must be protected from creation to disposal.

CSU Policy 8025.0, Privacy of Personal Information: Defines the rules governing the collection and storage of personal information.

CSU Standard, 8050.S100, Configuration Management: Defines encryption requirements for all devices that store confidential (level 1) data.

CSU Standard 8045.S400, Mobile Device Management: Defines requirements for storing confidential (level 1) data on a mobile device.

CSU Executive Order No. 1031, System-wide Records/Information Retention and Disposition: Defines the regulatory requirements and best practices of records/information retention and disposition.

What is Fresno State doing to ensure data security?

Our campus is in the process of implementing **2-Step Verification**, a system that requires a second method of verifying your identity, in addition to a username and password. This will ensure that your account, and the sensitive data you access, remain protected, even if your credentials are misplaced or stolen.

In addition, we we will soon deploy **Spirion**, a tool to protect sensitive data at Fresno State. The tool facilitates the discovery of confidential information stored on university systems. Knowing where all confidential data resides and taking any necessary remediation steps will help us maintain compliance with CSU and Fresno State security policies and standards.

As part of the University's efforts to raise security awareness, all Fresno State employees are required to complete a **50-minute security awareness course**. Managers, staff and student assistants will receive a notice of this training prior to the end of this semester. Faculty will

receive the training starting in the fall semester. This will better prepare us to fulfill our collective responsibility to safeguard sensitive data.

Lastly, institutions like Fresno State are regularly targeted by email "phishing" scams designed to obtain sensitive information. We will soon launch a program to help employees **recognize, report, and avoid phishing scams** that try to trick us into divulging confidential information.

How do I obtain additional information?

- You may view a complete list of CSU and Fresno State information security policies here.
- Fresno State retention and disposition schedules are available here.
- You may also contact Orlando Leon, Chief Information Officer at oleon@csufresno.edu.

Thank you for partnering with me to protect the sensitive data for which Fresno State is responsible.

Sincerely,

Joseph I. Castro, President