California State University Sacramento
College of Engineering and Computer Science

ECS Information Security Plan

Effective January 12, 2017

Preface

This document outlines the College of Engineering and Computer Science (ECS) plan to protect critical information and data, and to comply with all appropriate legal requirements regarding the same. To this end, the College maintains certain practices in the ECS information technology environment. The main units and/or persons impacted by these practices are the College's academic and administrative departments, and our faculty, staff and students.

This document's objectives are to:

- Define the College's Information Security Plan,
- Provide an outline to assure ongoing compliance with regulations related to this Plan, and
- Position the College for likely future privacy and security regulations.

Information Security Plan Coordination

ECS Computing Services is the organization within the College of Engineering and Computer Science tasked with the responsibility to coordinate and monitor the ECS Information Security Plan.

Risk Assessment and Safeguards

ECS Computing Services works with all relevant areas of the College to identify potential and actual risks to security and privacy of information. This is accomplished by:

- Periodic data security reviews,
- Identification of employees in their respective areas that work with sensitive data and information;
- Periodic reviews of procedures, incidents, and responses; and
- Publication of all relevant materials, except in those cases where publication may likely lead to breaches of security or privacy, for the purpose of educating the College community on network security and privacy issues.

While ECS Computing Services is generally responsible for the identification of internal and external risk assessment, all members of the College community are involved in risk assessment.

ECS Computing Services will:

- Monitor the network connections of all computers on the ECS network to protect its security and integrity.
- Maintain records and procedures of patching activity. ECS Computing Services provides patches for operating systems and software environments that are reasonably current.
- Keep current on potential threats to the network and its data, and will conduct risk assessments and regularly update them.
- Develop and maintain, with input from relevant College departments, a process for data recovery on relevant software systems
- Conduct audits of network activity and report significant questionable activities.
- Push forward with the goal of ensuring that sensitive electronic information is encrypted in transit and that ECS databases are strongly protected (now and in the future) from security risks.
- Assure the physical security of all ECS servers and terminals which contain or have access to sensitive data and information.

Employee Training and Education

Everyone in the College is ultimately responsible for ensuring their own compliance with information security practices. To aid in this, the College will develop training or education programs for all employees who have access to sensitive data.

Evaluation and Revision of the Information Security Plan

The ECS Information Security Plan will be subject to periodic review and adjustment. Reviews will occur as technology changes and evolving risks are identified. Review of processes in relevant offices of the College and the training or education program will also occur regularly. Periodic reevaluation of the plan itself, as well as the related data retention policy, should be conducted to assure ongoing compliance with existing and future laws and regulations.

Definitions

Sensitive data and information for the purpose of this plan includes faculty, staff and student personal information, including but not limited to Social Security Numbers. Covered data and information includes both paper and electronic records.