Information Security Plan

Redacted Version May 2022

Effective Date: 8/25/2021

Version History

Version #	Date	Contributor	Change Control
0.1	4/23/2018	ITSO	Initial Draft
0.7	05/30/2018	MCC	Merge Infiniti and MCC Comments
0.8	06/05/2018	MCC	MCC Updates / Questions
0.9	06/07/2018	MCC	Updates per Conference Call
v.10	06/14/2018	MCC	Proposed Changes
v.10	6/20/2018	MCC	Accepted Changes
V1.0	8/22/2018	MCC	Final Draft
V1.1	11/25/2019	Erich Donze	Initial 2019 Review
V1.2	7/15/2021	Erich Donze	Initial 2021 Review
V1.3	8/25/2021	ITSO	2021 Annual Review

Introduction

MiraCosta College's (MCC) Information Security Plan is the guiding publication where all organizational policies, processes, standards and employee expectations are documented as they relate to safeguarding Controlled Unclassified Information (CUI) and IT assets of MCC.

The National Institute of Standards and Technology's (NIST) Special Publication 800-171 provides the framework on which the policies and processes in this plan are based. Ensuring all electronic data is stored, processed, and discarded according to NIST's standards is a critical component of MCC's mission. As such, it is the responsibility of management, employees, and contractors at MCC to adhere to the policies and procedures outlined below.

While NIST 800-171 describe the use of CUI, MCC further decomposes data into categories of Public, Confidential, and Restricted information. When Public, Confidential and Restricted information are not explicitly referenced, the broader category of CUI is being described.

Unless otherwise indicated, "policy" refers to Academic Information Services (AIS) policy rather than District policy. If it is a board policy, we will refer to it in the document as a District Policy.

Within this document, you will find the NIST policies related to the following:

- **Access and Control** – establishes the rules for the access and use of the network infrastructure
- **Awareness and Training** – training on security policies, procedures, and technical security controls
- **Audit and Accountability** – ensures security controls are sufficient and effective
- **Configuration Management** – establishes the rules for the maintenance, expansion and use of the configuration and network infrastructure.
- **Identification and Authentication** – establishes access controls
- **Incident Response** – identifies incident response requirements
- **Maintenance** – establishes resource and maintenance requirements
- **Media and Systems Communication** – protection of information output
- **Personnel Security** – describes requirements that limit improper use of assets
- **Physical Protection** – identifies the measures that prevent physical unauthorized use or access
- **Risk Assessment** – describes the identification and review of critical processes
- **Security Assessment** – designates continuing efforts to ensure security objectives

- **System and Information Integrity** – defines ongoing efforts to ensure appropriate controls are maintained

The Information Technology Security Officer (ITSO) has reviewed and approved the document and is responsible for updating it annually. Additionally, ITSO will ensure the policies are implemented, that the staff are compliant with said policies, and that the appropriate steps are carried out in the event of an incident. For any questions related to this document, please contact:

Anthony Maciel
Associate Vice President/ Chief Information Systems Officer

MiraCosta College
(760) 795-6720
amaciel@miracosta.edu

Steve Schultz
Infrastructure Services & Systems Coordinator

MiraCosta College
(760) 795-6737
sschultz@miracosta.edu

Erich Donze
Information Security Engineer

MiraCosta College
(760) 795-6727
edonze@miracosta.edu

Table of Contents

Due to the sensitivity and confidential nature of the information contained within this document, the full document will be provided upon request.