



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

Introduction.....	3
Section 1 - Access Control.....	10
1.1 Overview	10
1.2 Purpose	10
1.3 Scope.....	11
1.4 Policy	11
1.5 Enforcement	15
1.6 Distribution	15
Section 2 – Awareness and Training.....	16
2.1 Overview	16
2.2 Purpose	16
2.3 Scope.....	16
2.4 Policy	17
2.5 Enforcement	18
2.6 Distribution	18
Section 3 - Audit and Accountability	20
3.1 Overview	20
3.2 Purpose	20
3.3 Scope.....	20
3.4 Policy	21
3.5 Enforcement	23
3.6 Distribution	23
Section 4 - Configuration Management.....	24
4.1 Overview	24
4.2 Purpose	24
4.3 Scope.....	25
4.4 Policy	25
4.5 Enforcement	29
4.6 Distribution	29
Section 5 - Identification and Authentication	30
5.1 Overview	30

5.2	Purpose.....	30
5.3	Scope	30
5.4	Policy	31
A.	NEW USER ACCOUNTS	32
B.	SELECTING PASSWORDS/PHRASES	32
C.	PASSWORD/PHRASE MINIMUM STANDARDS:	33
D.	PASSWORD/PHRASE GUIDELINES	34
E.	PASSWORD/PHRASE CHANGES	35
F.	SOFTWARE APPLICATIONS	35
5.5	Enforcement.....	35
5.6	Distribution.....	36
Section 6 - Incident Response		37
6.1	Overview	37
6.2	Purpose.....	37
6.3	Scope	37
6.4	Policy	38
A.	ESTABLISHMENT OF AN INCIDENT RESPONSE TEAM	38
B.	RISK ASSESSMENT CLASSIFICATION	39
C.	DOCUMENTATION AND COMMUNICATION OF INCIDENTS	40
D.	RESPONDER PROCEDURES	40
E.	SPECIAL SITUATIONS/EXCEPTIONS	41
F.	INCIDENT REPORTING	41
G.	TRAINING	41
6.5	Enforcement.....	42
6.6	Distribution.....	42
Section 7 - Maintenance		43
7.1	Overview	43
7.2	Purpose.....	43
7.3	Scope	43
7.4	Policy	44
A.	RESPONSIBILITY TO MAINTAIN FUNCTIONALITY	44
B.	SECURITY RESPONSIBILITIES	45
C.	RESPONSIBILITY TO CONDUCT PREVENTIVE MEASURES	46

D. RESPONSIBILITY TO PREVENT UNAUTHORIZED / INAPPROPRIATE ACCESS AND DISCLOSURE	47
E. PERMISSIBLE ACCESS BY DATA MANAGERS AND STAFF	48
F. INVESTIGATION OF MISCONDUCT	48
G. WHERE REQUIRED BY LAW	48
H. ACCESS FOR COWORKERS	49
I. RESPONSIBILITY FOR POLICY ADHERENCE	49
J. SYSTEM USER RESPONSIBILITIES	49
K. MAINTENANCE OF INFORMATION SYSTEMS	50
7.5 Enforcement.....	50
7.6 Distribution.....	50
Section 8 - Media and Systems Communications Protection.....	51
8.1 Overview	51
8.2 Purpose.....	52
8.3 Scope	52
8.4 Policy	52
A. MEDIA PROTECTION AND ACCESS	52
B. SYSTEM AND COMMUNICATION PROTECTIONS	53
C. MASS COMMUNICATIONS	54
8.5 Enforcement	55
8.6 Distribution.....	55
Section 9 - Personnel Security.....	56
9.1 Overview	56
9.2 Purpose.....	56
9.3 Scope	56
9.4 Policy	56
9.5 Enforcement	58
9.6 Distribution.....	58
Section 10 - Physical Protection	59
10.1 Overview	59
10.2 Purpose	59
10.3 Scope.....	59
10.4 Policy	59

10.5	Enforcement	63
10.6	Distribution	63
Section 11 - Risk Assessment		64
11.1	Overview	64
11.2	Purpose	64
11.3	Scope.....	64
11.4	Policy	65
A.	RISK ASSESSMENTS	65
B.	RISK ANALYSIS	66
C.	RISK TREATMENT PLAN	66
11.5	Enforcement	67
11.6	Distribution	67
Section 12 - Security Assessment.....		68
12.1	Overview	68
12.2	Purpose	68
A.	SECURITY OBJECTIVES	68
B.	SECURITY ASSESSMENT	69
12.3	Scope.....	69
12.4	Policy	69
A.	STATEMENT OF POSITION	69
B.	CLASSIFICATION	70
C.	NETWORK SEGMENTATION	70
D.	TRUSTED POINTS	70
E.	DATA IN TRANSIT	74
F.	CLASSIFICATIONS	75
I.	CLASSIFICATION OF DATA	75
II.	CLASSIFICATION OF USERS	75
III.	CLASSIFICATION OF EQUIPMENT	76
IV.	CLASSIFICATION OF NETWORKS	76
G.	RESPONSIBILITIES	76
H.	INFORMATION SYSTEM COMMUNICATIONS	79
12.5	Enforcement	80
12.6	Distribution.....	80

Section 13 - System and Information Integrity	81
13.1 Overview	81
13.2 Purpose	81
13.3 Scope	82
13.4 Policy	82
13.5 Enforcement	83
13.6 Distribution	83

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