System Security Plan

CMMC Level 2 Compliance

Prepared by: Cameron Koecher  
Date: 7/15/2024  
Version: 1.0



Disclaimer: This is a creative work intended for educational purposes at Dallas College. The contents of this document do not reflect an actual assessment or commentary on the cybersecurity posture of Dallas College or any real entity. All scenarios and analyses presented are hypothetical and designed solely for academic use.

# **Introduction**

## ****Purpose****

The purpose of this System Security Plan (SSP) is to outline the current state of cybersecurity controls and procedures within the Dallas College IT department in alignment with the requirements of CMMC Level 2. This document serves as a comprehensive guide to the security controls implemented to protect Controlled Unclassified Information (CUI) and to ensure compliance with federal cybersecurity standards.

## ****Scope****

This SSP covers all systems, networks, applications, and personnel involved in the handling and protection of CUI within the Dallas College IT department. The plan addresses both technical and administrative controls necessary to safeguard sensitive information.

## ****System Overview****

The IT systems at Dallas College include various components that support academic, administrative, and research activities. The primary systems covered in this plan include:

* **Network Infrastructure**: Routers, switches, firewalls, and intrusion detection systems (IDS).
* **Endpoints**: Workstations, laptops, mobile devices, and servers.
* **Applications**: Email services, cloud storage, student information systems, and collaboration tools.
* **Data Repositories**: Databases and file storage systems containing CUI.

# Security Controls

## ****Access Control (AC)****

* **Current State**: Access to systems containing CUI is currently controlled through username and password authentication. However, Multi-Factor Authentication (MFA) is not implemented.
* **Planned Improvements**: Implementation of MFA across all systems accessing CUI is scheduled to be completed within 90 days. An updated Access Control Policy will mandate MFA usage.

## ****Incident Response (IR)****

* **Current State**: The Incident Response Plan (IRP) is outdated, lacking specific procedures for incident detection, reporting, and communication.
* **Planned Improvements**: The IRP will be revised to include detailed incident handling steps, reporting channels, and communication protocols. A tabletop exercise is planned within 60 days to validate the new procedures.

## ****Audit and Accountability (AU)****

* **Current State**: Minimal logging is performed, and there is no regular review of audit logs. There is a lack of automated tools for log analysis.
* **Planned Improvements**: Enhanced logging capabilities and automated log analysis tools will be deployed within 60 days. A schedule for regular log reviews will be established to ensure timely detection of security incidents.

## ****Configuration Management (CM)****

* **Current State**: There is no formal Change Management Policy in place. System changes are managed informally without proper documentation or risk assessment.
* **Planned Improvements**: A formal Change Management Policy will be created to govern all changes to IT systems, ensuring that security controls are maintained. A change management tool will be implemented to track all changes.

## ****Data Protection (MP)****

* **Current State**: Data at rest and in transit is not currently encrypted, increasing the risk of unauthorized access and data breaches.
* **Planned Improvements**: Encryption solutions for data storage systems and communication channels will be deployed within 120 days. A Data Protection Policy will be developed to enforce encryption for all CUI.

## ****Identification and Authentication (IA)****

* **Current State**: User authentication is based on single-factor authentication (username and password).
* **Planned Improvements**: MFA will be implemented, and password policies will be strengthened to comply with CMMC requirements.

## ****Physical Protection (PE)****

* **Current State**: Physical access to critical systems is restricted to authorized personnel only, but monitoring is minimal.
* **Planned Improvements**: Physical security controls will be enhanced by installing additional surveillance cameras and access control mechanisms.

## ****System and Communications Protection (SC)****

* **Current State**: Network security is limited with minimal monitoring and no automated intrusion detection.
* **Planned Improvements**: Advanced network monitoring tools and intrusion detection systems (IDS) will be implemented to provide continuous monitoring and automated detection of potential threats.

## ****Personnel Security (PS)****

* **Current State**: Personnel security checks are conducted, but there is no continuous monitoring of personnel with access to CUI.
* **Planned Improvements**: A process for continuous monitoring and reassessment of personnel with access to CUI will be established.

## ****Training and Awareness (AT)****

* **Current State**: Annual cybersecurity training is conducted, but it lacks focus on CUI handling and advanced persistent threats (APTs).
* **Planned Improvements**: New training modules focusing on CUI handling and APT awareness will be developed and rolled out within 60 days. Training frequency will be increased to quarterly.

# Risk Assessment

## ****Risk Management Process****

* **Current State**: The last risk assessment was conducted three years ago, with no ongoing risk management process in place. This lack of a continuous risk management process leaves the department vulnerable to emerging threats and evolving risks.
* **Planned Improvements**: A comprehensive risk management process will be established to regularly evaluate and mitigate risks.

## ****Risk Assessment Procedures****

**Procedures**:

* + **Initial Risk Assessment**: Conduct an initial comprehensive risk assessment to identify and evaluate potential risks to CUI and other critical assets. This assessment will be completed within 30 days.
  + **Risk Categorization**: Risks will be categorized based on their impact and likelihood, using a risk matrix. This will help prioritize mitigation efforts.
  + **Risk Mitigation Strategies**: Develop and implement risk mitigation strategies based on the risk assessment findings. Strategies may include implementing new controls, enhancing existing controls, or accepting certain risks with documented justification.
  + **Continuous Risk Monitoring**: Establish a continuous risk monitoring process to regularly evaluate risks and adjust controls as needed. This will involve regular (quarterly) reviews of the risk register and updates to the risk management plan.

## ****Tools and Responsibilities****

* **Tools**: The department will use risk management tools such as FAIR and ISO 27005 to document and analyze risks. These tools will assist in maintaining an up-to-date risk register and in identifying potential new threats.
* **Responsibilities**: The Risk Management Team, led by the Chief Information Security Officer (CISO), will be responsible for conducting risk assessments, maintaining the risk register, and ensuring that risk mitigation strategies are implemented effectively.

# Continuous Monitoring and Maintenance

## ****Continuous Monitoring Plan****

* **Current State**: Limited continuous monitoring is currently in place, focusing primarily on manual reviews and ad hoc assessments. There is no formalized continuous monitoring strategy, and system maintenance practices are informal.
* **Planned Improvements**: A continuous monitoring plan will be developed to provide ongoing oversight of cybersecurity controls and ensure that they remain effective against current and emerging threats.

## ****Continuous Monitoring Procedures****

**Procedures**:

* **Deployment of Monitoring Tools**: Implement advanced monitoring tools, such as SIEM (Security Information and Event Management) systems, to provide real-time analysis of security alerts generated by network hardware and applications.
* **Automated Alerts and Responses**: Set up automated alerts for potential security incidents, enabling the IT security team to respond promptly to threats.
* **Regular Review and Analysis**: Conduct regular (e.g., daily, weekly) reviews of monitoring data to identify and respond to anomalies or potential security incidents.
* **Integration with Incident Response**: Ensure continuous monitoring efforts are integrated with the Incident Response Plan (IRP) to provide immediate action when threats are detected.

## ****Maintenance Activities****

**Activities**:

* + **Regular System Updates**: Schedule and perform regular system updates and patch management to address vulnerabilities and improve system security.
  + **Periodic Control Testing**: Conduct periodic testing of security controls (e.g., access controls, encryption, firewalls) to verify their effectiveness.
  + **Hardware and Software Inventory Management**: Maintain an up-to-date inventory of all hardware and software assets to ensure they are properly secured and monitored.

## ****Roles and Responsibilities****

* **Responsibilities**: The IT Operations Team, in coordination with the IT Security Team, will be responsible for implementing the continuous monitoring plan, conducting regular reviews, and ensuring that all maintenance activities are performed as scheduled.

# ****Summary****

The Dallas College IT department is committed to achieving and maintaining CMMC Level 2 compliance to protect Controlled Unclassified Information (CUI) and meet federal cybersecurity standards. This System Security Plan (SSP) has identified several gaps in the current cybersecurity posture, both in policy and technical controls, and outlined detailed remediation actions to address these deficiencies.

## ****Summary of Findings****

Throughout this plan, we have identified key areas where the current cybersecurity controls fall short of the CMMC Level 2 requirements:

* **Access Control**: Lack of Multi-Factor Authentication (MFA) and inadequate user access management pose risks of unauthorized access to sensitive information.
* **Incident Response**: An outdated Incident Response Plan (IRP) that does not meet current standards for incident handling and communication.
* **Data Protection**: Insufficient measures to protect CUI, including a lack of encryption for data at rest and in transit.
* **Network Security and Monitoring**: Limited network monitoring capabilities and a lack of automated tools for log analysis reduce the ability to detect and respond to potential threats.
* **Training and Awareness**: Existing cybersecurity training programs do not adequately address CUI handling and advanced persistent threats (APTs).
* **Risk Management**: An outdated risk assessment process and lack of continuous risk management increase the vulnerability to evolving threats.

## ****Commitment to Remediation and Continuous Improvement****

To address these gaps, the IT department will implement the remediation actions detailed in this SSP. Key initiatives include:

* **Deploying MFA and Updating Access Controls**: To enhance protection against unauthorized access.
* **Revamping the IRP**: To ensure timely and effective responses to cybersecurity incidents.
* **Enhancing Data Protection**: Through the implementation of encryption technologies and updated policies.
* **Improving Network Security**: By deploying advanced monitoring tools and automating log analysis.
* **Expanding Training Programs**: To improve staff awareness and preparedness against CUI-related threats and APTs.
* **Establishing Continuous Risk Management Practices**: To proactively identify and mitigate risks on an ongoing basis.

## ****Next Steps****

Moving forward, the Dallas College IT department will:

1. **Prioritize Remediation Efforts**: Focus on high-impact areas first, such as implementing MFA and updating the IRP.
2. **Allocate Resources and Assign Responsibilities**: Ensure that the appropriate teams are equipped with the necessary tools and training to carry out the remediation actions.
3. **Monitor and Validate Changes**: Conduct regular audits and assessments to validate the effectiveness of the implemented controls and adjust strategies as needed.
4. **Prepare for Official CMMC Assessment**: Once remediation actions are completed, perform a mock assessment to identify any remaining gaps and ensure readiness for an official CMMC Level 2 evaluation.
5. **Establish Ongoing Compliance Monitoring**: Implement continuous monitoring and periodic reviews to ensure sustained compliance and address emerging threats promptly.

## ****Long-Term Vision****

Achieving CMMC Level 2 compliance is not a one-time effort but an ongoing commitment to cybersecurity excellence. The IT department will continue to enhance its cybersecurity posture by:

* **Staying Informed on Cybersecurity Trends**: Regularly updating policies and practices based on the latest cybersecurity threats and regulatory changes.
* **Investing in Advanced Technologies**: Exploring and adopting new technologies that enhance threat detection and response capabilities.
* **Fostering a Culture of Security**: Encouraging all staff to prioritize cybersecurity in their daily activities and promoting a culture of vigilance and accountability.

## ****Conclusion****

By following the remediation actions outlined in this System Security Plan, the Dallas College IT department will significantly enhance its ability to protect CUI, maintain compliance with CMMC Level 2 requirements, and mitigate risks associated with cybersecurity threats. The commitment to continuous improvement and vigilance will ensure that Dallas College remains resilient against evolving cyber threats, safeguarding its information assets and supporting its mission of providing high-quality education and research.