System Security Plan

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for: Client Company

Prepared by: YourIT Company

System Security Plan

1 - Overview

We perform a periodic assessment of our information system environment with regards to the principals and functions set as part of the CMMC 2.0 - Level 2 and/or NIST 800-171 security control requirements. The assessment consists of automated scans in conjunction with a review by an Internal Assessor.

The System Security Plan document contains an overview of the NIST 800-171 Rev. 2 control requirements and the current state of compliance with the control requirements.

The methodology for the review and supporting documentation can be found in the various assessment reports and documents (referenced in the CMMC 2.0 - Level 2 Assessor Checklist or the NIST 800-171 Assessment). Issues are noted in the Plan of Action and Milestones report.

This document supplements the Risk Analysis, Risk Treatment Plan, and NIST SP 800-171 DoD Assessment Scoring report and offers substantiation and verification of compliance with control requirements.

System Name

myco.com

System Categorization

Medium

System Identifier

myco - 878D8CI23

Organization Responsible for Information System

Myco, Inc. 123 Ralston Drive Alpharetta, GA 30041 Tel: 770-555-1212

Information Owner

Hugh Laurie 123 Ralston Drive Alpharetta, GA 30041 Tel: 770-555-1212 Email: hlaurie@performanceit.com

System Owner

Warren Holdings, LLC Contact: Rowan Atkinson 123 Ralston Drive Alpharetta, GA 30041 Tel: 770-555-1212 Email: ratkinson@warrenholdingsllc.com

Function and Purpose

The purpose of the information system is to sell, deliver, support, and bill for DoD related services.

2 - System Environment

2.1 - System Environment

We have performed a System Inventory and Risk Assessment as part of our routine CMMC 2.0 - Level 2 and/or a NIST 800-171 Rev. 2 compliance review.

See the attached Technical Assessment report and Plan of Action and Milestones report.

SYSTEM NETWORK ASSESSMENT SUMMARY

LOCAL ACCOUNTS	
# Enabled	3
Last Login Within 30 Days	0
Last Login Older Than 30 Days	3
# Disabled	5
Last Login Within 30 Days	0
Last Login Older Than 30 Days	5

SECURITY GROUPS	
Groups with Users	0
# Total Groups	0

ACTIVE DIRECTORY COMPUTERS	
Total Computers	3

ACTIVE DIRECTORY COMPUTERS	
Last Login Within 30 Days	0
Last Login Older Than 30 Days	3

ACTIVE DIRECTORY COMPUTERS BY OS	
CentOS Linux release 7.3.1611 (Core)	1
Mac macOS 10.13.2 (17C88)	1
Windows 10 Enterprise	1

MISCELLANEOUS	
Non-A/D Systems	0
MX Records	0
MS SQL Servers	0
Web Servers	0
Printers	1
Exchange Servers	0
Network Shares	4
Installed Applications	37

2.2 - Computer Asset and Non-Active Directory Device Inventory

2.2.1 - System Hardware Inventory

Windows Computer Asset Inventory

An automated inventory of Windows computer assets in the network was performed as part of this assessment. The discovered assets can be seen in the Asset Inventory Review Worksheet and referenced in the Technical Assessment Report.

The details associated with each Windows computer can be seen in the Technical Assessment Report.

Non-Active Directory Device Inventory

An automated inventory of Non-Active Directory Device assets in the network was performed as part of this assessment. The discovered assets can be seen in the Non-AD Devices section contained within the Technical Assessment Report.

Printer Asset Inventory

An automated inventory of Printer assets in the network was performed as part of this assessment. The discovered assets can be seen in the Printers section of the Technical Assessment Report.

2.2.2 - Network Diagram

A network diagram has been included as part of this system security plan. Reference Myco information system network diagram.

2.2.3 - Software Application Inventory

An automated inventory of installed software was performed as part of this assessment. The discovered software applications can be seen in the Technical Assessment Report.

2.3 - System Boundaries

2.3.1 - External Information Systems

The following external information systems were catalogued as a part of this assessment:

Name	Description	Purpose	Business Owner	Criticality
Microsoft 365	Microsoft 365	Office Applications	CEO	Critical

2.3.2 - External IP Address and Port Use Summary

A technical assessment of external IP addresses, ports, and protocols has not been performed as part of this assessment.

2.3.3 - Web Servers

An automated inventory of Web Servers in the network was performed as part of this assessment. The discovered assets can be seen in the Web Servers section contained within the Technical Assessment Report.

2.3.4 - Local Mail Servers

An automated inventory of Local Mail Servers in the network was performed as part of this assessment. The discovered assets can be seen in the Local Mail Servers section contained within the Technical Assessment Report.

2.4 - Hardware and Software Maintenance and Ownership

The system hardware and software are maintained and owned by the System Owner referenced in Section 1 - Overview of this System Security Plan.

3 - System Security Requirements

3.1 - Access Control

3.1.1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization limits system access to authorized users, processes acting on behalf of authorized users, and devices (including other information systems).

3.1.2. Limit system access to the types of transactions and functions that authorized users are permitted to execute.

☐ Implemented ☑ Planned to be Implemented ☐ Not Applicable

Our organization plans to implement this control requirement per the plan detailed below.

Comments:

No comments.

Action Plan Milestones:

The organization will implement measures to limit access in accordance with this requirement's policy.

The actions planned to meet this requirement noted in the Plan of Action and Milestones Report.

3.1.3. Control the flow of CUI in accordance with approved authorizations.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization controls the flow of CUI in accordance with approved authorizations.

3.1.4. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization will separates the duties of individuals to reduce the risk of malevolent activity without collusion The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.1.5. Employ the principle of least privilege, including for specific security functions and privileged accounts

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization employs the principle of least privilege, including for specific security functions and privileged accounts. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.1.6. Use non-privileged accounts or roles when accessing nonsecurity functions.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization uses non-privileged accounts or roles when accessing non-security functions. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.1.7. Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization prevents non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.1.8. Limit unsuccessful logon attempts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has not implemented this control requirement.

Comments:

No comments.

The issue is noted in the Plan of Action and Milestones Report.

3.1.9. Provide privacy and security notices consistent with applicable CUI rules.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization provides privacy and security notices consistent with applicable CUI rules. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.1.10. Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization uses session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.1.11. Terminate (automatically) a user session after a defined condition.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization terminates (automatically) a user session after a defined condition. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.1.12. Monitor and control remote access sessions.

☐ Implemented ☑ Planned to be Implemented ☐ Not Applicable

Our organization plans to implement this control requirement per the plan detailed below.

Comments:

No comments.

Action Plan Milestones:

The organization will implement measures to monitor and control remote access in accordance with this requirement's policy.

The actions planned to meet this requirement noted in the Plan of Action and Milestones Report.

3.1.13. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

Policy The organization employs cryptographic mechanisms to protect the confidentiality of remote access sessions. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.1.14. Route remote access via managed access control points.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization routes remote access via managed access control points. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.1.15. Authorize remote execution of privileged commands and remote access to security-relevant information.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization authorizes remote execution of privileged commands and remote access to security-relevant information. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.1.16. Authorize wireless access prior to allowing such connections.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

No comments.

3.1.17. Protect wireless access using authentication and encryption.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization protects wireless access using authentication and encryption. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.1.18. Control connection of mobile devices.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization protects wireless access using authentication and encryption. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.1.19. Encrypt CUI on mobile devices and mobile computing platforms.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization encrypts CUI on mobile devices and mobile computing platforms. (Mobile devices and mobile computing platforms include, for example, smartphones, tablets, E-readers, and notebook computers.) The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.1.20. Verify and control/limit connections to and use of external systems.

☐ Implemented ☑ Planned to be Implemented ☐ Not Applicable

Our organization plans to implement this control requirement per the plan detailed below.

Comments:

No comments.

Action Plan Milestones:

The organization will implement measures to limit external connections in accordance with this requirement's policy.

The actions planned to meet this requirement noted in the Plan of Action and Milestones Report.

3.1.21. Limit use of organizational portable storage devices on external systems.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization limits use of organizational portable storage devices on external systems. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.1.22. Control CUI posted or processed on publicly accessible systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has not implemented this control requirement.

Comments:

No comments.

The issue is noted in the Plan of Action and Milestones Report.

3.2 - Awareness and Training

3.2.1. Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization ensures that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.2.2. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization ensures that personnel are trained to carry out their assigned information security-related duties and responsibilities. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.2.3. Provide security awareness training on recognizing and reporting potential indicators of insider threat.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has not implemented this control requirement.

Comments:

No comments.

The issue is noted in the Plan of Action and Milestones Report.

3.3 - Audit and Accountability

3.3.1. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization creates and retains system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. The purpose is to implement policies and procedures for defining audit requirements. This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.3.2. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization ensures that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. The purpose is to implement policies and procedures for defining audit requirements. This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.3.3. Review and update logged events.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has not implemented this control requirement.

Comments:

No comments.

The issue is noted in the Plan of Action and Milestones Report.

3.3.4. Alert in the event of an audit logging process failure.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization reviews and updates logged events. The purpose is to implement policies and procedures for reviewing logs of access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.3.5. Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has not implemented this control requirement.

Comments:

No comments.

The issue is noted in the Plan of Action and Milestones Report.

3.3.6. Provide audit record reduction and report generation to support on-demand analysis and reporting.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has not implemented this control requirement.

Comments:

No comments.

The issue is noted in the Plan of Action and Milestones Report.

3.3.7. Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization provides a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. The purpose is to implement policies and procedures for granting access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.3.8. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization protects audit information and audit logging tools from unauthorized access, modification, and deletion. The purpose is to implement policies and procedures for logging access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.3.9. Limit management of audit logging functionality to a subset of privileged users.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

The organization limits management of audit logging functionality to a subset of privileged users. The purpose is to implement policies and procedures for logging access to Controlled Unclassified Information (CUI). This policy applies to all organization workforce members and all systems, network, and applications that process, store or transmit CUI. This policy also applies to all vendors, partners, and contractors.

3.4 - Configuration Management

3.4.1. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has not implemented this control requirement.

Comments:

No comments.

The issue is noted in the Plan of Action and Milestones Report.

3.4.2. Establish and enforce security configuration settings for information technology products employed in organizational systems.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

No comments.

3.4.3. Track, review, approve or disapprove, and log changes to organizational systems.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

No comments.

3.4.4. Analyze the security impact of changes prior to implementation.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

No comments.

3.4.5. Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

No comments.

3.4.6. Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

No comments.

3.4.7. Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

No comments.

3.4.8. Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

No comments.

3.4.9. Control and monitor user-installed software.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

No comments.

3.5 - Identification and Authentication

3.5.1. Identify system users, processes acting on behalf of users, and devices.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

No comments.

3.5.2. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

☑ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has implemented this control requirement using the methodology presented below.

Comments:

No comments.

3.5.3. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

☐ Implemented ☑ Planned to be Implemented ☐ Not Applicable

Our organization plans to implement this control requirement per the plan detailed below.

Comments:

No comments.

Action Plan Milestones:

The organization will implement Multifactor Authentication in accordance with this requirement's policy.

The actions planned to meet this requirement noted in the Plan of Action and Milestones Report.

3.5.4. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Our organization has not implemented this control requirement.

Comments:

No comments.

The issue is noted in the Plan of Action and Milestones Report.

Truncated Sample Report