PreVeil Customer Responsibility Matrix
Controls and Objectives

PREVEIL PROPRIETARY

Assumption: All CUI data will be transmitted and stored using PreVeil, only.
The customer is responsible for determining which controls are applicable, and for developing and maintaining the customer SSP as well as policies, procedures, and supplemental documentation required for compliance related to assessments and audits.
PreVeil claims no responsibility or liability regarding customers information, effort, and execution of their compliance related tasks.
NOTE: The responses contained within this document are specific to PreVeil and the customer's instance of PreVeil. This document does not address any other systems or endpoints that may be considered in scope for a PreVeil customer's assessment.

Control/Objectives Status Legend

Shared	In addition to the customer responsibilities listed in the assumptions and notes statements above, there will be some customer responsibility within the control/objective. This can include, but not limited to, additional documentation, end point management activities, application/system scanning, administrative management activities, asset management, etc. PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way.
PreVeil Inherited	As long as all assumptions and notes above are understood and addressed, PreVeil addresses the control/objective. Note: the customer may still have outstanding responsibilities, based on their internal business processes, technology infrastructure, CUI/FCI handling processes, and/or end point management activities (i.e., ensuring Bitlocker or other hard drive encryption methods are used for any laptop/desktop processing, transmitting, and/or storing CUI). PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information as to how PreVeil manages controls marked in this way for PreVeil customers.
Customer Responsibility	The customer will be reponsible for the objective/control marked "Customer Responsibility". PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way.

Practice Area	CMMC Practice	NIST SP 800-171	Objective/Control	Practice Statement/Objective	Control/Objective Status
Access Control (AC)	AC.L1-3.1.1	3.1.1	Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Shared
Access Control (AC)	AC.L1-3.1.1(a)	3.1.1(a)	Objective	Authorized users are identified	Shared
Access Control (AC)	AC.L1-3.1.1(b)	3.1.1(b)	Objective	Processes acting on behalf of authorized users are identified	PreVeil Inherited
Access Control (AC)	AC.L1-3.1.1(c)	3.1.1(c)	Objective	Devices (and other systems) authorized to connect to the system are identified	PreVeil Inherited
Access Control (AC)	AC.L1-3.1.1(d)	3.1.1(d)	Objective	System access is limited to authorized users	Shared
Access Control (AC)	AC.L1-3.1.1(e)	3.1.1(e)	Objective	System access is limited to processes acting on behalf of authorized users	PreVeil Inherited
Access Control (AC)	AC.L1-3.1.1(f)	3.1.1(f)	Objective	System access is limited to authorized devices (including other systems)	Shared
Access Control (AC)	AC.L1-3.1.2	3.1.2	Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	PreVeil Inherited
Access Control (AC)	AC.L1-3.1.2(a)	3.1.2(a)	Objective	The types of transactions and functions that authorized users are permitted to execute are defined	PreVeil Inherited
Access Control (AC)	AC.L1-3.1.2(b)	3.1.2(b)	Objective	System access is limited to the defined types of transactions and functions for authorized users	PreVeil Inherited
Access Control (AC)	AC.L1-3.1.20	3.1.20	Control	Verify and control/limit connections to and use of external information systems.	Shared
Access Control (AC)	AC.L1-3.1.20(a)	3.1.20(a)	Objective	Connections to external systems are identified	Shared
Access Control (AC)	AC.L1-3.1.20(b)	3.1.20(b)	Objective	The use of external systems is identified	Shared
Access Control (AC)	AC.L1-3.1.20(c)	3.1.20(c)	Objective	Connections to external systems are verified	Shared
Access Control (AC)	AC.L1-3.1.20(d)	3.1.20(d)	Objective	The use of external systems is verified	Shared
Access Control (AC)	AC.L1-3.1.20(e)	3.1.20(e)	Objective	Connections to external systems are controlled/limited	Shared
Access Control (AC)	AC.L1-3.1.20(f)	3.1.20(f)	Objective	The use of external systems is controlled/limited	Shared
Access Control (AC)	AC.L1-3.1.22	3.1.22	Control	Control information posted or processed on publicly accessible information systems.	Customer Responsibility
Access Control (AC)	AC.L1-3.1.22(a)	3.1.22(a)	Objective	Individuals authorized to post or process information on publicly accessible systems are identified	Customer Responsibility
Access Control (AC)	AC.L1-3.1.22(b)	3.1.22(b)	Objective	Procedures to ensure FCI is not posted or processed on publicly accessible systems are identified	Customer Responsibility
Access Control (AC)	AC.L1-3.1.22(c)	3.1.22(c)	Objective	A review process is in place prior to posting of any content to publicly accessible systems	Customer Responsibility
Access Control (AC)	AC.L1-3.1.22(d)	3.1.22(d)	Objective	Content on publicly accessible systems is reviewed to ensure that it does not include FCI	Customer Responsibility
Access Control (AC)	AC.L1-3.1.22(e)	3.1.22(e)	Objective	Mechanisms are in place to remove and address improper posting of FCI	Customer Responsibility
Access Control (AC)	AC.L2-3.1.3	3.1.3	Control	Control the flow of CUI in accordance with approved authorizations.	Shared
Access Control (AC)	AC.L2-3.1.3(a)	3.1.3(a)	Objective	Information flow control policies are defined	Customer Responsibility
Access Control (AC)	AC.L2-3.1.3(b)	3.1.3(b)	Objective	Methods and enforcement mechanisms for controlling the flow of CUI are defined	Shared
Access Control (AC)	AC.L2-3.1.3(c)	3.1.3(c)	Objective	Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified;	Shared
Access Control (AC)	AC.L2-3.1.3(d)	3.1.3(d)	Objective	Authorizations for controlling the flow of CUI are defined	Customer Responsibility
Access Control (AC)	AC.L2-3.1.3(e)	3.1.3(e)	Objective	Approved authorizations for controlling the flow of CUI are enforced	Shared
Access Control (AC)	AC.L2-3.1.4	3.1.4	Control	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Shared
Access Control (AC)	AC.L2-3.1.4(a)	3.1.4(a)	Objective	The duties of individuals requiring separation are defined	Customer Responsibility
Access Control (AC)	AC.L2-3.1.4(b)	3.1.4(b)	Objective	Responsibilities for duties that require separation are assigned to separate individuals	Shared
Access Control (AC)	AC.L2-3.1.4(c)	3.1.4(c)	Objective	Access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals	Shared
Access Control (AC)	AC.L2-3.1.5	3.1.5	Control	Employ principle of least privilege, including for specific security functions and privileged accounts.	Shared
Access Control (AC)	AC.L2-3.1.5(a)	3.1.5(a)	Objective	Privileged accounts are identified	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.5(b)	3.1.5(b)	Objective	Access to privileged accounts is authorized in accordance with the principle of least privilege	Shared
Access Control (AC)	AC.L2-3.1.5(c)	3.1.5(c)	Objective	Security functions are identified	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.5(d)	3.1.5(d)	Objective	Access to security functions is authorized in accordance with the principle of least privilege	Shared
Access Control (AC)	AC.L2-3.1.6	3.1.6	Control	Use non-privileged accounts or roles when accessing nonsecurity functions.	Shared
Access Control (AC)	AC.L2-3.1.6(a)	3.1.6(a)	Objective	Nonsecurity functions are identified	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.6(b)	3.1.6(b)	Objective	Users are required to use non-privileged accounts or roles when accessing nonsecurity functions	Shared
Access Control (AC)	AC.L2-3.1.7	3.1.7	Control	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.7(a)	3.1.7(a)	Objective	Privileged functions are defined	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.7(b)	3.1.7(b)	Objective	Non-privileged users are defined	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.7(c)	3.1.7(c)	Objective	Non-privileged users are prevented from executing privileged functions	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.7(d)	3.1.7(d)	Objective	The execution of privileged functions is captured in audit logs	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.8	3.1.8	Control	Limit unsuccessful logon attempts.	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.8(a)	3.1.8(a)	Objective	The means of limiting unsuccessful logon attempts is defined	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.8(b)	3.1.8(b)	Objective	The defined means of limiting unsuccessful logon attempts is implemented	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.9	3.1.9	Control	Provide privacy and security notices consistent with CUI rules.	Shared
Access Control (AC)	AC.L2-3.1.9(a)	3.1.9(a)	Objective	Privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category	Shared
Access Control (AC)	AC.L2-3.1.9(b)	3.1.9(b)	Objective	Privacy and security notices are displayed	Shared
Access Control (AC)	AC.L2-3.1.10	3.1.10	Control	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	Customer Responsibility
Access Control (AC)	AC.L2-3.1.10(a)	3.1.10(a)	Objective	The period of inactivity after which the system initiates a session lock is defined	Customer Responsibility
Access Control (AC)	AC.L2-3.1.10(b)	3.1.10(b)	Objective	Access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity;	Customer Responsibility
Access Control (AC)	AC.L2-3.1.10(c)	3.1.10(c)	Objective	Previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.	Customer Responsibility
Access Control (AC)	AC.L2-3.1.11	3.1.11	Control	Terminate (automatically) user sessions after a defined condition.	Shared
Access Control (AC)	AC.L2-3.1.11(a)	3.1.11(a)	Objective	Conditions requiring a user session to terminate are defined	Shared
Access Control (AC)	AC.L2-3.1.11(b)	3.1.11(b)	Objective	A user session is automatically terminated after any of the defined conditions occur	Shared
Access Control (AC)	AC.L2-3.1.12	3.1.12	Control	Monitor and control remote access sessions.	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.12(a)	3.1.12(a)	Objective	Remote access sessions are permitted	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.12(b)	3.1.12(b)	Objective	The types of permitted remote access are identified	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.12(c)	3.1.12(c)	Objective	Remote access sessions are controlled	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.12(d)	3.1.12(d)	Objective	Remote access sessions are monitored	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.13	3.1.13	Control	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.13(a)	3.1.13(a)	Objective	Cryptographic mechanisms to protect the confidentiality of remote access sessions are identified;	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.13(b)	3.1.13(b)	Objective	Cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.14	3.1.14	Control	Route remote access via managed access control points.	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.14(a)	3.1.14(a)	Objective	Managed access control points are identified and implemented	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.14(b)	3.1.14(b)	Objective	Remote access is routed through managed network access control points	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.15	3.1.15	Control	Authorize remote execution of privileged commands and remote access to security-relevant information.	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.15(a)	3.1.15(a)	Objective	Privileged commands authorized for remote execution are identified	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.15(b)	3.1.15(b)	Objective	Security-relevant information authorized to be accessed remotely is identified	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.15(c)	3.1.15(c)	Objective	The execution of the identified privileged commands via remote access is authorized	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.15(d)	3.1.15(d)	Objective	Access to the identified security-relevant information via remote access is authorized	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.16	3.1.16	Control	Authorize wireless access prior to allowing such connections.	Customer Responsibility
Access Control (AC)	AC.L2-3.1.16(a)	3.1.16(a)	Objective	Wireless access points are identified	Customer Responsibility
Access Control (AC)	AC.L2-3.1.16(b)	3.1.16(b)	Objective	Wireless access is authorized prior to allowing such connections	Customer Responsibility

PreVeil Customer Responsibility Matrix Controls and Objectives

PREVEIL PROPRIETARY

Assumption: All CUI data will be transmitted and stored using PreVeil, only.

The customer is responsible for determining which controls are applicable, and for developing and maintaining the customer SSP as well as policies, procedures, and supplemental documentation required for compliance related to assessments and audits.

PreVeil claims no responsibility or liability regarding customers information, effort, and execution of their compliance related tasks.

NOTE: The responses contained within this document are specific to PreVeil and the customer's instance of PreVeil. This document does not address any other systems or endpoints that may be considered in scope for a PreVeil customer's assessment.

Control/Objectives Status Legend

Shared	In addition to the customer responsibilities listed in the assumptions and notes statements above, there will be some customer responsibility within the control/objective. This can include, but not limited to, additional documentation, end point management activities, application/system scanning, administrative management activities, asset management, etc. PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way.
PreVeil Inherited	As long as all assumptions and notes above are understood and addressed, PreVeil addresses the control/objective. Note: the customer may still have outstanding responsibilities, based on their internal business processes, technology infrastructure, CUI/FCI handling processes, and/or end point management activities (i.e., ensuring Bitlocker or other hard drive encryption methods are used for any laptop/desktop processing, transmitting, and/or storing CUI). PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information as to how PreVeil manages controls marked in this way for PreVeil customers.
Customer Responsibility	The customer will be reponsible for the objective/control marked "Customer Responsibility". PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way.

Practice Area	CMMC Practice	NIST SP 800-171	Objective/Control	Practice Statement/Objective	Control/Objective Status
Access Control (AC)	AC.L2-3.1.17	3.1.17	Control	Protect wireless access using authentication and encryption.	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.17(a)	3.1.17(a)	Objective	Wireless access to the system is protected using authentication	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.17(b)	3.1.17(b)	Objective	Wireless access to the system is protected using encryption	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.18	3.1.18	Control	Control connection of mobile devices.	Shared
Access Control (AC)	AC.L2-3.1.18(a)	3.1.18(a)	Objective	Mobile devices that process, store, or transmit CUI are identified	Customer Responsibility
Access Control (AC)	AC.L2-3.1.18(b)	3.1.18(b)	Objective	Mobile device connections are authorized	Shared
Access Control (AC)	AC.L2-3.1.18(c)	3.1.18(c)	Objective	Mobile device connections are monitored and logged	Shared
Access Control (AC)	AC.L2-3.1.19	3.1.19	Control	Encrypt CUI on mobile devices and mobile computing platforms.	Shared
Access Control (AC)	AC.L2-3.1.19(a)	3.1.19(a)	Objective	Mobile devices and mobile computing platforms that process, store, or transmit CUI are identified	Shared
Access Control (AC)	AC.L2-3.1.19(b)	3.1.19(b)	Objective	Encryption is employed to protect CUI on identified mobile devices and mobile computing platforms	PreVeil Inherited
Access Control (AC)	AC.L2-3.1.21	3.1.21	Control	Limit use of portable storage devices on external systems.	Shared
Access Control (AC)	AC.L2-3.1.21(a)	3.1.21(a)	Objective	The use of portable storage devices containing CUI on external systems is identified and documented	Shared
Access Control (AC)	AC.L2-3.1.21(b)	3.1.21(b)	Objective	Limits on the use of portable storage devices containing CUI on external systems are defined	Shared
Access Control (AC)	AC.L2-3.1.21(c)	3.1.21(c)	Objective	The use of portable storage devices containing CUI on external systems is limited as defined.	Shared
Awareness and Training (AT)	AT.L1-3.2.1	3.2.1	Control	Ensure that managers, system 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.	Shared
Awareness and Training (AT)	AT.L1-3.2.1(a)	3.2.1(a)	Objective	Security risks associated with organizational activities involving CUI are identified	Shared
Awareness and Training (AT)	AT.L1-3.2.1(b)	3.2.1(b)	Objective	Policies, standards, and procedures related to the security of the system are identified	Customer Responsibility
Awareness and Training (AT)	AT.L1-3.2.1(c)	3.2.1(c)	Objective	Managers, systems administrators, and users of the system are made aware of the security risks associated with their activities	Shared
Awareness and Training (AT)	AT.L1-3.2.1(d)	3.2.1(d)	Objective	Managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system	Customer Responsibility
Awareness and Training (AT)	AT.L2-3.2.2	3.2.2	Control	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	Shared
Awareness and Training (AT)	AT.L2-3.2.2(a)	3.2.2(a)	Objective	Information security-related duties, roles, and responsibilities are defined	Shared
Awareness and Training (AT)	AT.L2-3.2.2(b)	3.2.2(b)	Objective	Information security-related duties, roles, and responsibilities are assigned to designated personnel;	Customer Responsibility
Awareness and Training (AT)	AT.L2-3.2.2(c)	3.2.2(c)	Objective	Personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities	Shared
Awareness and Training (AT)	AT.L2-3.2.3	3.2.3	Control	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Shared
Awareness and Training (AT)	AT.L2-3.2.3(a)	3.2.3(a)	Objective	Potential indicators associated with insider threats are identified	Shared
Awareness and Training (AT)	AT.L2-3.2.3(b)	3.2.3(b)	Objective	Security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees	Shared
Audit and Accountability (AU)	AU.L2-3.3.1	3.3.1	Control	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.	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.1(a)	3.3.1(a)	Objective	Audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.1(b)	3.3.1(b)	Objective	The content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.1(c)	3.3.1(c)	Objective	Audit records are created (generated)	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.1(d)	3.3.1(d)	Objective	Audit records, once created, contain the defined content	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.1(e)	3.3.1(e)	Objective	Retention requirements for audit records are defined	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.1(f)	3.3.1(f)	Objective	Audit records are retained as defined	Shared
Audit and Accountability (AU)	AU.L2-3.3.2	3.3.2	Control	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.2(a)	3.3.2(a)	Objective	The content of the audit records needed to support the ability to uniquely trace users to their actions is defined	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.2(b)	3.3.2(b)	Objective	Audit records, once created, contain the defined content.	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.3	3.3.3	Control	Review and update logged events.	Shared
Audit and Accountability (AU)	AU.L2-3.3.3(a)	3.3.3(a)	Objective	A process for determining when to review logged events is defined	Customer Responsibility
Audit and Accountability (AU)	AU.L2-3.3.3(b)	3.3.3(b)	Objective	Event types being logged are reviewed in accordance with the defined review process	Shared
Audit and Accountability (AU)	AU.L2-3.3.3(c)	3.3.3(c)	Objective	Event types being logged are updated based on the review.	Shared
Audit and Accountability (AU)	AU.L2-3.3.4	3.3.4	Control	Alert in the event of an audit logging process failure.	Shared
Audit and Accountability (AU)	AU.L2-3.3.4(a)	3.3.4(a)	Objective	Personnel or roles to be alerted in the event of an audit logging process failure are identified	Shared
Audit and Accountability (AU)	AU.L2-3.3.4(b)	3.3.4(b)	Objective	Types of audit logging process failures for which alert will be generated are defined	Shared
Audit and Accountability (AU)	AU.L2-3.3.4(c)	3.3.4(c)	Objective	Identified personnel or roles are alerted in the event of an audit logging process failure	Customer Responsibility
Audit and Accountability (AU)	AU.L2-3.3.5	3.3.5	Control	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Shared
Audit and Accountability (AU)	AU.L2-3.3.5(a)	3.3.5(a)	Objective	Audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined	Shared
Audit and Accountability (AU)	AU.L2-3.3.5(b)	3.3.5(b)	Objective	Defined audit record review, analysis, and reporting processes are correlated	Shared
Audit and Accountability (AU)	AU.L2-3.3.6	3.3.6	Control	Provide audit record reduction and report generation to support on-demand analysis and reporting.	Shared
Audit and Accountability (AU)	AU.L2-3.3.6(a)	3.3.6(a)	Objective	An audit record reduction capability that supports on-demand analysis is provided	Shared
Audit and Accountability (AU)	AU.L2-3.3.6(b)	3.3.6(b)	Objective	A report generation capability that supports on-demand reporting is provided	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.7	3.3.7	Control	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.7(a)	3.3.7(a)	Objective	Internal system clocks are used to generate time stamps for audit records	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.7(b)	3.3.7(b)	Objective	An authoritative source with which to compare and synchronize internal system clocks is specified	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.7(c)	3.3.7(c)	Objective	Internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.8	3.3.8	Control	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Shared
Audit and Accountability (AU)	AU.L2-3.3.8(a)	3.3.8(a)	Objective	Audit information is protected from unauthorized access	Shared
Audit and Accountability (AU)	AU.L2-3.3.8(b)	3.3.8(b)	Objective	Audit information is protected from unauthorized modification	Shared
Audit and Accountability (AU)	AU.L2-3.3.8(c)	3.3.8(c)	Objective	Audit information is protected from unauthorized deletion	Shared
Audit and Accountability (AU)	AU.L2-3.3.8(d)	3.3.8(d)	Objective	Audit logging tools are protected from unauthorized access	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.8(e)	3.3.8(e)	Objective	Audit logging tools are protected from unauthorized modification	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.8(f)	3.3.8(f)	Objective	Audit logging tools are protected from unauthorized deletion	PreVeil Inherited
Audit and Accountability (AU)	AU.L2-3.3.9	3.3.9	Control	Limit management of audit logging functionality to a subset of privileged users.	Shared
Audit and Accountability (AU)	AU.L2-3.3.9(a)	3.3.9(a)	Objective	A subset of privileged users granted access to manage audit logging functionality is defined	Shared
Audit and Accountability (AU)	AU.L2-3.3.9(b)	3.3.9(b)	Objective	Management of audit logging functionality is limited to the defined subset of privileged users.	Shared

PreVeil Customer Responsibility Matrix
Controls and Objectives

PREVEIL PROPRIETARY

Assumption: All CUI data will be transmitted and stored using PreVeil, only.

The customer is responsible for determining which controls are applicable, and for developing and maintaining the customer SSP as well as policies, procedures, and supplemental documentation required for compliance related to assessments and audits.

PreVeil claims no responsibility or liability regarding customers information, effort, and execution of their compliance related tasks.

NOTE: The responses contained within this document are specific to PreVeil and the customer's instance of PreVeil. This document does not address any other systems or endpoints that may be considered in scope for a PreVeil customer's assessment.

Control/Objectives Status Legend

Shared	In addition to the customer responsibilities listed in the assumptions and notes statements above, there will be some customer responsibility within the control/objective. This can include, but not limited to, additional documentation, end point management activities, application/system scanning, administrative management activities, asset management, etc. PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way.
PreVeil Inherited	As long as all assumptions and notes above are understood and addressed, PreVeil addresses the control/objective. Note: the customer may still have outstanding responsibilities, based on their internal business processes, technology infrastructure, CUI/FCI handling processes, and/or end point management activities (i.e., ensuring Bitlocker or other hard drive encryption methods are used for any laptop/desktop processing, transmitting, and/or storing CUI). PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information as to how PreVeil manages controls marked in this way for PreVeil customers.
Customer Responsibility	The customer will be reponsible for the objective/control marked "Customer Responsibility". PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way.

Practice Area	CMMC Practice	NIST SP 800-171	Objective/Control	Practice Statement/Objective	Control/Objective Status
Configuration Management (CM)	CM.L2-3.4.1	3.4.1	Control	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Shared
Configuration Management (CM)	CM.L2-3.4.1(a)	3.4.1(a)	Objective	A baseline configuration is established	Shared
Configuration Management (CM)	CM.L2-3.4.1(b)	3.4.1(b)	Objective	The baseline configuration includes hardware, software, firmware, and documentation	Shared
Configuration Management (CM)	CM.L2-3.4.1(c)	3.4.1(c)	Objective	The baseline configuration is maintained (reviewed and updated) throughout the system development life cycle	Shared
Configuration Management (CM)	CM.L2-3.4.1(d)	3.4.1(d)	Objective	A system inventory is established	Shared
Configuration Management (CM)	CM.L2-3.4.1(e)	3.4.1(e)	Objective	The system inventory includes hardware, software, firmware, and documentation	Shared
Configuration Management (CM)	CM.L2-3.4.1(f)	3.4.1(f)	Objective	The inventory is maintained (reviewed and updated) throughout the system development life cycle	Shared
Configuration Management (CM)	CM.L2-3.4.2	3.4.2	Control	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Shared
Configuration Management (CM)	CM.L2-3.4.2(a)	3.4.2(a)	Objective	Security configuration settings for information technology products employed in the system are established and included in the baseline configuration	Shared
Configuration Management (CM)	CM.L2-3.4.2(b)	3.4.2(b)	Objective	Security configuration settings for information technology products employed in the system are enforced	Shared
Configuration Management (CM)	CM.L2-3.4.3	3.4.3	Control	Track, review, approve, or disapprove, and log changes to organizational systems.	Shared
Configuration Management (CM)	CM.L2-3.4.3(a)	3.4.3(a)	Objective	Changes to the system are tracked	Shared
Configuration Management (CM)	CM.L2-3.4.3(b)	3.4.3(b)	Objective	Changes to the system are reviewed	Shared
Configuration Management (CM)	CM.L2-3.4.3(c)	3.4.3(c)	Objective	Changes to the system are approved or disapproved	Shared
Configuration Management (CM)	CM.L2-3.4.3(d)	3.4.3(d)	Objective	Changes to the system are logged	Shared
Configuration Management (CM)	CM.L2-3.4.4	3.4.4	Control	Analyze the security impact of changes prior to implementation.	Shared
Configuration Management (CM)	CM.L2-3.4.4(a)	3.4.4(a)	Objective	The security impact of changes to the system is analyzed prior to implementation	Shared
Configuration Management (CM)	CM.L2-3.4.5	3.4.5	Control	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	Shared
Configuration Management (CM)	CM.L2-3.4.5(a)	3.4.5(a)	Objective	Physical access restrictions associated with changes to the system are defined	PreVeil Inherited
Configuration Management (CM)	CM.L2-3.4.5(b)	3.4.5(b)	Objective	Physical access restrictions associated with changes to the system are documented	PreVeil Inherited
Configuration Management (CM)	CM.L2-3.4.5(c)	3.4.5(c)	Objective	Physical access restrictions associated with changes to the system are approved	PreVeil Inherited
Configuration Management (CM)	CM.L2-3.4.5(d)	3.4.5(d)	Objective	Physical access restrictions associated with changes to the system are enforced	PreVeil Inherited
Configuration Management (CM)	CM.L2-3.4.5(e)	3.4.5(e)	Objective	Logical access restrictions associated with changes to the system are defined	Shared
Configuration Management (CM)	CM.L2-3.4.5(f)	3.4.5(f)	Objective	Logical access restrictions associated with changes to the system are documented	Shared
Configuration Management (CM)	CM.L2-3.4.5(g)	3.4.5(g)	Objective	Logical access restrictions associated with changes to the system are approved	Shared
Configuration Management (CM)	CM.L2-3.4.5(h)	3.4.5(h)	Objective	Logical access restrictions associated with changes to the system are enforced	Shared
Configuration Management (CM)	CM.L2-3.4.6	3.4.6	Control	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Shared
Configuration Management (CM)	CM.L2-3.4.6(a)	3.4.6(a)	Objective	Essential system capabilities are defined based on the principle of least functionality	Shared
Configuration Management (CM)	CM.L2-3.4.6(b)	3.4.6(b)	Objective	The system is configured to provide only the defined essential capabilities	PreVeil Inherited
Configuration Management (CM)	CM.L2-3.4.7	3.4.7	Control	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	Shared
Configuration Management (CM)	CM.L2-3.4.7(a)	3.4.7(a)	Objective	Essential programs are defined	Customer Responsibility
Configuration Management (CM)	CM.L2-3.4.7(b)	3.4.7(b)	Objective	The use of nonessential programs is defined	Customer Responsibility
Configuration Management (CM)	CM.L2-3.4.7(c)	3.4.7(c)	Objective	The use of nonessential programs is restricted, disabled, or prevented as defined	Shared
Configuration Management (CM)	CM.L2-3.4.7(d)	3.4.7(d)	Objective	Essential functions are defined	Customer Responsibility
Configuration Management (CM)	CM.L2-3.4.7(e)	3.4.7(e)	Objective	The use of nonessential functions is defined	Customer Responsibility
Configuration Management (CM)	CM.L2-3.4.7(f)	3.4.7(f)	Objective	The use of nonessential functions is restricted, disabled, or prevented as defined	Shared
Configuration Management (CM)	CM.L2-3.4.7(g)	3.4.7(g)	Objective	Essential ports are defined	Customer Responsibility
Configuration Management (CM)	CM.L2-3.4.7(h)	3.4.7(h)	Objective	The use of nonessential ports is defined	Customer Responsibility
Configuration Management (CM)	CM.L2-3.4.7(i)	3.4.7(i)	Objective	The use of nonessential ports is restricted, disabled, or prevented as defined	Shared
Configuration Management (CM)	CM.L2-3.4.7(j)	3.4.7(j)	Objective	Essential protocols are defined	Customer Responsibility
Configuration Management (CM)	CM.L2-3.4.7(k)	3.4.7(k)	Objective	The use of nonessential protocols is defined	Customer Responsibility
Configuration Management (CM)	CM.L2-3.4.7(l)	3.4.7(l)	Objective	The use of nonessential protocols is restricted, disabled, or prevented as defined	Shared
Configuration Management (CM)	CM.L2-3.4.7(m)	3.4.7(m)	Objective	Essential services are defined	Customer Responsibility
Configuration Management (CM)	CM.L2-3.4.7(n)	3.4.7(n)	Objective	The use of nonessential services is defined	Customer Responsibility
Configuration Management (CM)	CM.L2-3.4.7(o)	3.4.7(o)	Objective	The use of nonessential services is restricted, disabled, or prevented as defined	Shared
Configuration Management (CM)	CM.L2-3.4.8	3.4.8	Control	Apply deny-by-exception (deny listing) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (allow listing) policy to allow the execution of authorized software.	Shared
Configuration Management (CM)	CM.L2-3.4.8(a)	3.4.8(a)	Objective	A policy specifying whether allow-listing or deny-listing is to be implemented is specified	Shared
Configuration Management (CM)	CM.L2-3.4.8(b)	3.4.8(b)	Objective	The software allowed to execute under allow-listing or denied use under deny-listing is specified	Shared
Configuration Management (CM)	CM.L2-3.4.8(c)	3.4.8(c)	Objective	Allow-listing to allow the execution of authorized software or deny-listing to prevent the use of unauthorized software is implemented as specified	Shared
Configuration Management (CM)	CM.L2-3.4.9	3.4.9	Control	Control and monitor user-installed software.	Shared
Configuration Management (CM)	CM.L2-3.4.9(a)	3.4.9(a)	Objective	A policy for controlling the installation of software by users is established	Shared
Configuration Management (CM)	CM.L2-3.4.9(b)	3.4.9(b)	Objective	Installation of software by users is controlled based on the established policy	Shared
Configuration Management (CM)	CM.L2-3.4.9(c)	3.4.9(c)	Objective	Installation of software by users is monitored	Shared
Identification and Authentication (IA)	IA.L1-3.5.1	3.5.1	Control	Identify information system users, processes acting on behalf of users, or devices.	Shared
Identification and Authentication (IA)	IA.L1-3.5.1(a)	3.5.1(a)	Objective	System users are identified	Shared
Identification and Authentication (IA)	IA.L1-3.5.1(b)	3.5.1(b)	Objective	Processes acting on behalf of users are identified	PreVeil Inherited
Identification and Authentication (IA)	IA.L1-3.5.1(c)	3.5.1(c)	Objective	Devices accessing the system are identified	Shared
Identification and Authentication (IA)	IA.L1-3.5.2	3.5.2	Control	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	PreVeil Inherited
Identification and Authentication (IA)	IA.L1-3.5.2(a)	3.5.2(a)	Objective	The identity of each user is authenticated or verified as a prerequisite to system access	PreVeil Inherited
Identification and Authentication (IA)	IA.L1-3.5.2(b)	3.5.2(b)	Objective	The identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access	PreVeil Inherited
Identification and Authentication (IA)	IA.L1-3.5.2(c)	3.5.2(c)	Objective	The identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access	PreVeil Inherited
Identification and Authentication (IA)	IA.L2-3.5.3	3.5.3	Control	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Shared
Identification and Authentication (IA)	IA.L2-3.5.3(a)	3.5.3(a)	Objective	Privileged accounts are identified	PreVeil Inherited
Identification and Authentication (IA)	IA.L2-3.5.3(b)	3.5.3(b)	Objective	Multifactor authentication is implemented for local access to privileged accounts	Customer Responsibility
Identification and Authentication (IA)	IA.L2-3.5.3(c)	3.5.3(c)	Objective	Multifactor authentication is implemented for network access to privileged accounts	Customer Responsibility
Identification and Authentication (IA)	IA.L2-3.5.3(d)	3.5.3(d)	Objective	Multifactor authentication is implemented for network access to non-privileged accounts	Customer Responsibility
Identification and Authentication (IA)	IA.L2-3.5.4	3.5.4	Control	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	PreVeil Inherited
Identification and Authentication (IA)	IA.L2-3.5.4(a)	3.5.4(a)	Objective	Replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts	PreVeil Inherited

PreVeil Customer Responsibility Matrix
Controls and Objectives

PREVEIL PROPRIETARY

Assumption: All CUI data will be transmitted and stored using PreVeil, only.

The customer is responsible for determining which controls are applicable, and for developing and maintaining the customer SSP as well as policies, procedures, and supplemental documentation required for compliance related to assessments and audits.

PreVeil claims no responsibility or liability regarding customers information, effort, and execution of their compliance related tasks.

NOTE: The responses contained within this document are specific to PreVeil and the customer's instance of PreVeil. This document does not address any other systems or endpoints that may be considered in scope for a PreVeil customer's assessment.

Control/Objectives Status Legend

Shared	In addition to the customer responsibilities listed in the assumptions and notes statements above, there will be some customer responsibility within the control/objective. This can include, but not limited to, additional documentation, end point management activities, application/system scanning, administrative management activities, asset management, etc. PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way.
PreVeil Inherited	As long as all assumptions and notes above are understood and addressed, PreVeil addresses the control/objective. Note: the customer may still have outstanding responsibilities, based on their internal business processes, technology infrastructure, CUI/FCI handling processes, and/or end point management activities (i.e., ensuring Bitlocker or other hard drive encryption methods are used for any laptop/desktop processing, transmitting, and/or storing CUI). PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information as to how PreVeil manages controls marked in this way for PreVeil customers.
Customer Responsibility	The customer will be reponsible for the objective/control marked "Customer Responsibility". PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way.

Practice Area	CMMC Practice	NIST SP 800-171	Objective/Control	Practice Statement/Objective	Control/Objective Status
Identification and Authentication (IA)	IA.L2-3.5.5	3.5.5	Control	Prevent the reuse of identifiers for a defined period.	Shared
Identification and Authentication (IA)	IA.L2-3.5.5(a)	3.5.5(a)	Objective	A period within which identifiers cannot be reused is defined	Shared
Identification and Authentication (IA)	IA.L2-3.5.5(b)	3.5.5(b)	Objective	Reuse of identifiers is prevented within the defined period	Shared
Identification and Authentication (IA)	IA.L2-3.5.6	3.5.6	Control	Disable identifiers after a defined period of inactivity.	Shared
Identification and Authentication (IA)	IA.L2-3.5.6(a)	3.5.6(a)	Objective	A period of inactivity after which an identifier is disabled is defined	Shared
Identification and Authentication (IA)	IA.L2-3.5.6(b)	3.5.6(b)	Objective	Identifiers are disabled after the defined period of inactivity	Shared
Identification and Authentication (IA)	IA.L2-3.5.7	3.5.7	Control	Enforce a minimum password complexity and change of characters when new passwords are created.	Shared
Identification and Authentication (IA)	IA.L2-3.5.7(a)	3.5.7(a)	Objective	Password complexity requirements are defined	Shared
Identification and Authentication (IA)	IA.L2-3.5.7(b)	3.5.7(b)	Objective	Password change of character requirements are defined	Shared
Identification and Authentication (IA)	IA.L2-3.5.7(c)	3.5.7(c)	Objective	Minimum password complexity requirements as defined are enforced when new passwords are created	Shared
Identification and Authentication (IA)	IA.L2-3.5.7(d)	3.5.7(d)	Objective	Minimum password change of character requirements as defined are enforced when new passwords are created	Shared
Identification and Authentication (IA)	IA.L2-3.5.8	3.5.8	Control	Prohibit password reuse for a specified number of generations.	Shared
Identification and Authentication (IA)	IA.L2-3.5.8(a)	3.5.8(a)	Objective	The number of generations during which a password cannot be reused is specified	Shared
Identification and Authentication (IA)	IA.L2-3.5.8(b)	3.5.8(b)	Objective	Reuse of passwords is prohibited during the specified number of generations	Shared
Identification and Authentication (IA)	IA.L2-3.5.9	3.5.9	Control	Allow temporary password use for system logons with an immediate change to a permanent password.	Shared
Identification and Authentication (IA)	IA.L2-3.5.9(a)	3.5.9(a)	Objective	An immediate change to a permanent password is required when a temporary password is used for system logon	Shared
Identification and Authentication (IA)	IA.L2-3.5.10	3.5.10	Control	Store and transmit only cryptographically-protected passwords.	Shared
Identification and Authentication (IA)	IA.L2-3.5.10(a)	3.5.10(a)	Objective	Passwords are cryptographically protected in storage	Shared
Identification and Authentication (IA)	IA.L2-3.5.10(b)	3.5.10(b)	Objective	Passwords are cryptographically protected in transit	Shared
Identification and Authentication (IA)	IA.L2-3.5.11	3.5.11	Control	Obscure feedback of authentication information.	Shared
Identification and Authentication (IA)	IA.L2-3.5.11(a)	3.5.11(a)	Objective	Authentication information is obscured during the authentication process	Shared
Incident Response (IR)	IR.L2-3.6.1	3.6.1	Control	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Shared
Incident Response (IR)	IR.L2-3.6.1(a)	3.6.1(a)	Objective	An operational incident-handling capability is established	Shared
Incident Response (IR)	IR.L2-3.6.1(b)	3.6.1(b)	Objective	The operational incident-handling capability includes preparation	Customer Responsibility
Incident Response (IR)	IR.L2-3.6.1(c)	3.6.1(c)	Objective	The operational incident-handling capability includes detection	Shared
Incident Response (IR)	IR.L2-3.6.1(d)	3.6.1(d)	Objective	The operational incident-handling capability includes analysis	Customer Responsibility
Incident Response (IR)	IR.L2-3.6.1(e)	3.6.1(e)	Objective	The operational incident-handling capability includes containment	Shared
Incident Response (IR)	IR.L2-3.6.1(f)	3.6.1(f)	Objective	The operational incident-handling capability includes recovery	Shared
Incident Response (IR)	IR.L2-3.6.1(g)	3.6.1(g)	Objective	The operational incident-handling capability includes user response activities	Shared
Incident Response (IR)	IR.L2-3.6.2	3.6.2	Control	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Customer Responsibility
Incident Response (IR)	IR.L2-3.6.2(a)	3.6.2(a)	Objective	Incidents are tracked	Customer Responsibility
Incident Response (IR)	IR.L2-3.6.2(b)	3.6.2(b)	Objective	Incidents are documented	Customer Responsibility
Incident Response (IR)	IR.L2-3.6.2(c)	3.6.2(c)	Objective	Authorities to whom incidents are to be reported are identified	Customer Responsibility
Incident Response (IR)	IR.L2-3.6.2(d)	3.6.2(d)	Objective	Organizational officials to whom incidents are to be reported are identified	Customer Responsibility
Incident Response (IR)	IR.L2-3.6.2(e)	3.6.2(e)	Objective	Identified authorities are notified of incidents	Customer Responsibility
Incident Response (IR)	IR.L2-3.6.2(f)	3.6.2(f)	Objective	Identified organizational officials are notified of incidents	Customer Responsibility
Incident Response (IR)	IR.L2-3.6.3	3.6.3	Control	Test the organizational incident response capability.	Customer Responsibility
Incident Response (IR)	IR.L2-3.6.3(a)	3.6.3(a)	Objective	The incident response capability is tested	Customer Responsibility
Maintenance (MA)	MA.L2-3.7.1	3.7.1	Control	Perform maintenance on organizational systems.	PreVeil Inherited
Maintenance (MA)	MA.L2-3.7.1(a)	3.7.1(a)	Objective	System maintenance is performed	PreVeil Inherited
Maintenance (MA)	MA.L2-3.7.2	3.7.2	Control	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	PreVeil Inherited
Maintenance (MA)	MA.L2-3.7.2(a)	3.7.2(a)	Objective	Tools used to conduct system maintenance are controlled	PreVeil Inherited
Maintenance (MA)	MA.L2-3.7.2(b)	3.7.2(b)	Objective	Techniques used to conduct system maintenance are controlled	PreVeil Inherited
Maintenance (MA)	MA.L2-3.7.2(c)	3.7.2(c)	Objective	Mechanisms used to conduct system maintenance are controlled	PreVeil Inherited
Maintenance (MA)	MA.L2-3.7.2(d)	3.7.2(d)	Objective	Personnel used to conduct system maintenance are controlled	PreVeil Inherited
Maintenance (MA)	MA.L2-3.7.3	3.7.3	Control	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Shared
Maintenance (MA)	MA.L2-3.7.3(a)	3.7.3(a)	Objective	Equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI	Shared
Maintenance (MA)	MA.L2-3.7.4	3.7.4	Control	Check media containing diagnostic and test programs for malicious code before the media is used in organizational systems.	PreVeil Inherited
Maintenance (MA)	MA.L2-3.7.4(a)	3.7.4(a)	Objective	Media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI	PreVeil Inherited
Maintenance (MA)	MA.L2-3.7.5	3.7.5	Control	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	PreVeil Inherited
Maintenance (MA)	MA.L2-3.7.5(a)	3.7.5(a)	Objective	Multifactor authentication is used to establish nonlocal maintenance sessions via external network connections	PreVeil Inherited
Maintenance (MA)	MA.L2-3.7.5(b)	3.7.5(b)	Objective	Nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete	PreVeil Inherited
Maintenance (MA)	MA.L2-3.7.6	3.7.6	Control	Supervise the maintenance activities of personnel without required access authorization.	PreVeil Inherited
Maintenance (MA)	MA.L2-3.7.6(a)	3.7.6(a)	Objective	Maintenance personnel without required access authorization are supervised during maintenance activities.	PreVeil Inherited
Media Protection (MP)	MP.L1-3.8.3	3.8.3	Control	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	Shared
Media Protection (MP)	MP.L1-3.8.3(a)	3.8.3(a)	Objective	System media containing FCI is sanitized or destroyed before disposal	Shared
Media Protection (MP)	MP.L1-3.8.3(b)	3.8.3(b)	Objective	System media containing FCI is sanitized before it is released for reuse	Shared
Media Protection (MP)	MP.L2-3.8.1	3.8.1	Control	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	Shared
Media Protection (MP)	MP.L2-3.8.1(a)	3.8.1(a)	Objective	Paper media containing CUI is physically controlled	Customer Responsibility
Media Protection (MP)	MP.L2-3.8.1(b)	3.8.1(b)	Objective	Digital media containing CUI is physically controlled	Shared
Media Protection (MP)	MP.L2-3.8.1(c)	3.8.1(c)	Objective	Paper media containing CUI is securely stored	Customer Responsibility
Media Protection (MP)	MP.L2-3.8.1(d)	3.8.1(d)	Objective	Digital media containing CUI is securely stored	Shared
Media Protection (MP)	MP.L2-3.8.2	3.8.2	Control	Limit access to CUI on system media to authorized users.	Shared
Media Protection (MP)	MP.L2-3.8.2(a)	3.8.2(a)	Objective	Access to CUI on system media is limited to authorized users	Shared
Media Protection (MP)	MP.L2-3.8.4	3.8.4	Control	Mark media with necessary CUI markings and distribution limitations.	Shared
Media Protection (MP)	MP.L2-3.8.4(a)	3.8.4(a)	Objective	Media containing CUI is marked with applicable CUI markings	Shared
Media Protection (MP)	MP.L2-3.8.4(b)	3.8.4(b)	Objective	Media containing CUI is marked with distribution limitations	Shared

PreVeil Customer Responsibility Matrix
Controls and Objectives

PREVEIL PROPRIETARY

Assumption: All CUI data will be transmitted and stored using PreVeil, only.

The customer is responsible for determining which controls are applicable, and for developing and maintaining the customer SSP as well as policies, procedures, and supplemental documentation required for compliance related to assessments and audits.

PreVeil claims no responsibility or liability regarding customers information, effort, and execution of their compliance related tasks.

NOTE: The responses contained within this document are specific to PreVeil and the customer's instance of PreVeil. This document does not address any other systems or endpoints that may be considered in scope for a PreVeil customer's assessment.

Control/Objectives Status Legend

Shared	In addition to the customer responsibilities listed in the assumptions and notes statements above, there will be some customer responsibility within the control/objective. This can include, but not limited to, additional documentation, end point management activities, application/system scanning, administrative management activities, asset management, etc. PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way.
PreVeil Inherited	As long as all assumptions and notes above are understood and addressed, PreVeil addresses the control/objective. Note: the customer may still have outstanding responsibilities, based on their internal business processes, technology infrastructure, CUI/FCI handling processes, and/or end point management activities (i.e., ensuring Bitlocker or other hard drive encryption methods are used for any laptop/desktop processing, transmitting, and/or storing CUI). PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information as to how PreVeil manages controls marked in this way for PreVeil customers.
Customer Responsibility	The customer will be reponsible for the objective/control marked "Customer Responsibility". PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way.

Practice Area	CMMC Practice	NIST SP 800-171	Objective/Control	Practice Statement/Objective	Control/Objective Status
Media Protection (MP)	MP.L2-3.8.5	3.8.5	Control	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	Shared
Media Protection (MP)	MP.L2-3.8.5(a)	3.8.5(a)	Objective	Access to media containing CUI is controlled	Shared
Media Protection (MP)	MP.L2-3.8.5(b)	3.8.5(b)	Objective	Accountability for media containing CUI is maintained during transport outside of controlled areas	Shared
Media Protection (MP)	MP.L2-3.8.6	3.8.6	Control	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	Shared
Media Protection (MP)	MP.L2-3.8.6(a)	3.8.6(a)	Objective	The confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical	Shared
Media Protection (MP)	MP.L2-3.8.7	3.8.7	Control	Control the use of removable media on system components.	Shared
Media Protection (MP)	MP.L2-3.8.7(a)	3.8.7(a)	Objective	The use of removable media on system components is controlled	Shared
Media Protection (MP)	MP.L2-3.8.8	3.8.8	Control	Prohibit the use of portable storage devices when such devices have no identifiable owner.	Shared
Media Protection (MP)	MP.L2-3.8.8(a)	3.8.8(a)	Objective	The use of portable storage devices is prohibited when such devices have no identifiable owner	Shared
Media Protection (MP)	MP.L2-3.8.9	3.8.9	Control	Protect the confidentiality of backup CUI at storage locations.	Shared
Media Protection (MP)	MP.L2-3.8.9(a)	3.8.9(a)	Objective	The confidentiality of backup CUI is protected at storage locations	Shared
Personnel Security (PS)	PS.L2-3.9.1	3.9.1	Control	Screen individuals prior to authorizing access to organizational systems containing CUI.	Shared
Personnel Security (PS)	PS.L2-3.9.1(a)	3.9.1(a)	Objective	Individuals are screened prior to authorizing access to organizational systems containing CUI	Shared
Personnel Security (PS)	PS.L2-3.9.2	3.9.2	Control	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Shared
Personnel Security (PS)	PS.L2-3.9.2(a)	3.9.2(a)	Objective	A policy and/or process for terminating system access and any credentials coincident with personnel actions is established	Customer Responsibility
Personnel Security (PS)	PS.L2-3.9.2(b)	3.9.2(b)	Objective	System access and credentials are terminated consistent with personnel actions such as termination or transfer	Shared
Personnel Security (PS)	PS.L2-3.9.2(c)	3.9.2(c)	Objective	The system is protected during and after personnel transfer actions	Shared
Physical Protection (PE)	PE.L1-3.10.1	3.10.1	Control	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	PreVeil Inherited
Physical Protection (PE)	PE.L1-3.10.1(a)	3.10.1(a)	Objective	Authorized individuals allowed physical access are identified	PreVeil Inherited
Physical Protection (PE)	PE.L1-3.10.1(b)	3.10.1(b)	Objective	Physical access to organizational systems is limited to authorized individuals	PreVeil Inherited
Physical Protection (PE)	PE.L1-3.10.1(c)	3.10.1(c)	Objective	Physical access to equipment is limited to authorized individuals	PreVeil Inherited
Physical Protection (PE)	PE.L1-3.10.1(d)	3.10.1(d)	Objective	Physical access to operating environments is limited to authorized individuals	PreVeil Inherited
Physical Protection (PE)	PE.L1-3.10.3	3.10.3	Control	Escort visitors and monitor visitor activity.	PreVeil Inherited
Physical Protection (PE)	PE.L1-3.10.3(a)	3.10.3(a)	Objective	Visitors are escorted	PreVeil Inherited
Physical Protection (PE)	PE.L1-3.10.3(b)	3.10.3(b)	Objective	Visitor activity is monitored	PreVeil Inherited
Physical Protection (PE)	PE.L1-3.10.4	3.10.4	Control	Maintain audit logs of physical access.	PreVeil Inherited
Physical Protection (PE)	PE.L1-3.10.4(a)	3.10.4(a)	Objective	Audit logs of physical access are maintained	PreVeil Inherited
Physical Protection (PE)	PE.L1-3.10.5	3.10.5	Control	Control and manage physical access devices.	PreVeil Inherited
Physical Protection (PE)	PE.L1-3.10.5(a)	3.10.5(a)	Objective	Physical access devices are identified	PreVeil Inherited
Physical Protection (PE)	PE.L1-3.10.5(b)	3.10.5(b)	Objective	Physical access devices are controlled	PreVeil Inherited
Physical Protection (PE)	PE.L1-3.10.5(c)	3.10.5(c)	Objective	Physical access devices are managed	PreVeil Inherited
Physical Protection (PE)	PE.L2-3.10.2	3.10.2	Control	Protect and monitor the physical facility and support infrastructure for organizational systems.	PreVeil Inherited
Physical Protection (PE)	PE.L2-3.10.2(a)	3.10.2(a)	Objective	The physical facility where organizational systems reside is protected	PreVeil Inherited
Physical Protection (PE)	PE.L2-3.10.2(b)	3.10.2(b)	Objective	The support infrastructure for organizational systems is protected	PreVeil Inherited
Physical Protection (PE)	PE.L2-3.10.2(c)	3.10.2(c)	Objective	The physical facility where organizational systems reside is monitored	PreVeil Inherited
Physical Protection (PE)	PE.L2-3.10.2(d)	3.10.2(d)	Objective	The support infrastructure for organizational systems is monitored	PreVeil Inherited
Physical Protection (PE)	PE.L2-3.10.6	3.10.6	Control	Enforce safeguarding measures for CUI at alternate work sites.	PreVeil Inherited
Physical Protection (PE)	PE.L2-3.10.6(a)	3.10.6(a)	Objective	Safeguarding measures for CUI are defined for alternate work sites	PreVeil Inherited
Physical Protection (PE)	PE.L2-3.10.6(b)	3.10.6(b)	Objective	Safeguarding measures for CUI are enforced for alternate work sites	PreVeil Inherited
Risk Assessment (RM)	RA.L2-3.11.1	3.11.1	Control	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	Shared
Risk Assessment (RM)	RA.L2-3.11.1(a)	3.11.1(a)	Objective	The frequency to assess risk to organizational operations, organizational assets, and individuals is defined	Shared
Risk Assessment (RM)	RA.L2-3.11.1(b)	3.11.1(b)	Objective	Risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency	Shared
Risk Assessment (RM)	RA.L2-3.11.2	3.11.2	Control	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Shared
Risk Assessment (RM)	RA.L2-3.11.2(a)	3.11.2(a)	Objective	The frequency to scan for vulnerabilities in organizational systems and applications is defined	Shared
Risk Assessment (RM)	RA.L2-3.11.2(b)	3.11.2(b)	Objective	Vulnerability scans are performed on organizational systems with the defined frequency	Shared
Risk Assessment (RM)	RA.L2-3.11.2(c)	3.11.2(c)	Objective	Vulnerability scans are performed on applications with the defined frequency	Shared
Risk Assessment (RM)	RA.L2-3.11.2(d)	3.11.2(d)	Objective	Vulnerability scans are performed on organizational systems when new vulnerabilities are identified	Shared
Risk Assessment (RM)	RA.L2-3.11.2(e)	3.11.2(e)	Objective	Vulnerability scans are performed on applications when new vulnerabilities are identified	Shared
Risk Assessment (RM)	RA.L2-3.11.3	3.11.3	Control	Remediate vulnerabilities in accordance with risk assessments.	Shared
Risk Assessment (RM)	RA.L2-3.11.3(a)	3.11.3(a)	Objective	Vulnerabilities are identified	Shared
Risk Assessment (RM)	RA.L2-3.11.3(b)	3.11.3(b)	Objective	Vulnerabilities are remediated in accordance with risk assessments	Shared
Security Assessment (CA)	CA.L2-3.12.1	3.12.1	Control	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Shared
Security Assessment (CA)	CA.L2-3.12.1(a)	3.12.1(a)	Objective	The frequency of security control assessments is defined	Shared
Security Assessment (CA)	CA.L2-3.12.1(b)	3.12.1(b)	Objective	Security controls are assessed with the defined frequency to determine if the controls are effective in their application	Shared
Security Assessment (CA)	CA.L2-3.12.2	3.12.2	Control	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Shared
Security Assessment (CA)	CA.L2-3.12.2(a)	3.12.2(a)	Objective	Deficiencies and vulnerabilities to be addressed by the plan of action are identified	Shared
Security Assessment (CA)	CA.L2-3.12.2(b)	3.12.2(b)	Objective	A plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities	Shared
Security Assessment (CA)	CA.L2-3.12.2(c)	3.12.2(c)	Objective	The plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities	Shared
Security Assessment (CA)	CA.L2-3.12.3	3.12.3	Control	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Shared
Security Assessment (CA)	CA.L2-3.12.3(a)	3.12.3(a)	Objective	Security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls	Shared
Security Assessment (CA)	CA.L2-3.12.4	3.12.4	Control	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	Customer Responsibility
Security Assessment (CA)	CA.L2-3.12.4(a)	3.12.4(a)	Objective	A system security plan is developed	Customer Responsibility

PreVeil Customer Responsibility Matrix
Controls and Objectives

PREVEIL PROPRIETARY

Assumption: All CUI data will be transmitted and stored using PreVeil, only.
The customer is responsible for determining which controls are applicable, and for developing and maintaining the customer SSP as well as policies, procedures, and supplemental documentation required for compliance related to assessments and audits.
PreVeil claims no responsibility or liability regarding customers information, effort, and execution of their compliance related tasks.
NOTE: The responses contained within this document are specific to PreVeil and the customer's instance of PreVeil. This document does not address any other systems or endpoints that may be considered in scope for a PreVeil customer's assessment.

Control/Objectives Status Legend

Shared	In addition to the customer responsibilities listed in the assumptions and notes statements above, there will be some customer responsibility within the control/objective. This can include, but not limited to, additional documentation, end point management activities, application/system scanning, administrative management activities, asset management, etc. PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way.
PreVeil Inherited	As long as all assumptions and notes above are understood and addressed, PreVeil addresses the control/objective. Note: the customer may still have outstanding responsibilities, based on their internal business processes, technology infrastructure, CUI/FCI handling processes, and/or end point management activities (i.e., ensuring Bitlocker or other hard drive encryption methods are used for any laptop/desktop processing, transmitting, and/or storing CUI). PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information as to how PreVeil manages controls marked in this way for PreVeil customers.
Customer Responsibility	The customer will be reponsible for the objective/control marked "Customer Responsibility". PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way.

Practice Area	CMMC Practice	NIST SP 800-171	Objective/Control	Practice Statement/Objective	Control/Objective Status
Security Assessment (CA)	CA.L2-3.12.4(b)	3.12.4(b)	Objective	The system boundary is described and documented in the system security plan	Customer Responsibility
Security Assessment (CA)	CA.L2-3.12.4(c)	3.12.4(c)	Objective	The system environment of operation is described and documented in the system security plan	Customer Responsibility
Security Assessment (CA)	CA.L2-3.12.4(d)	3.12.4(d)	Objective	The security requirements identified and approved by the designated authority as non-applicable are identified;	Customer Responsibility
Security Assessment (CA)	CA.L2-3.12.4(e)	3.12.4(e)	Objective	The method of security requirement implementation is described and documented in the system security plan	Customer Responsibility
Security Assessment (CA)	CA.L2-3.12.4(f)	3.12.4(f)	Objective	The relationship with or connection to other systems is described and documented in the system security plan	Customer Responsibility
Security Assessment (CA)	CA.L2-3.12.4(g)	3.12.4(g)	Objective	The frequency to update the system security plan is defined	Customer Responsibility
Security Assessment (CA)	CA.L2-3.12.4(h)	3.12.4(h)	Objective	System security plan is updated with the defined frequency	Customer Responsibility
System and Communications Protection (SC)	SC.L1-3.13.1	3.13.1	Control	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Shared
System and Communications Protection (SC)	SC.L1-3.13.1(a)	3.13.1(a)	Objective	The external system boundary is defined	Customer Responsibility
System and Communications Protection (SC)	SC.L1-3.13.1(b)	3.13.1(b)	Objective	Key internal system boundaries are defined	Customer Responsibility
System and Communications Protection (SC)	SC.L1-3.13.1(c)	3.13.1(c)	Objective	Communications are monitored at the external system boundary	Shared
System and Communications Protection (SC)	SC.L1-3.13.1(d)	3.13.1(d)	Objective	Communications are monitored at key internal boundaries	Shared
System and Communications Protection (SC)	SC.L1-3.13.1(e)	3.13.1(e)	Objective	Communications are controlled at the external system boundary	Shared
System and Communications Protection (SC)	SC.L1-3.13.1(f)	3.13.1(f)	Objective	Communications are controlled at key internal boundaries	Shared
System and Communications Protection (SC)	SC.L1-3.13.1(g)	3.13.1(g)	Objective	Communications are protected at the external system boundary	Shared
System and Communications Protection (SC)	SC.L1-3.13.1(h)	3.13.1(h)	Objective	Communications are protected at key internal boundaries	Shared
System and Communications Protection (SC)	SC.L1-3.13.5	3.13.5	Control	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Shared
System and Communications Protection (SC)	SC.L1-3.13.5(a)	3.13.5(a)	Objective	Publicly accessible system components are identified	Customer Responsibility
System and Communications Protection (SC)	SC.L1-3.13.5(b)	3.13.5(b)	Objective	Subnetworks for publicly accessible system components are physically or logically separated from internal networks	Shared
System and Communications Protection (SC)	SC.L2-3.13.2	3.13.2	Control	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.2(a)	3.13.2(a)	Objective	Architectural designs that promote effective information security are identified	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.2(b)	3.13.2(b)	Objective	Software development techniques that promote effective information security are identified	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.2(c)	3.13.2(c)	Objective	Systems engineering principles that promote effective information security are identified	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.2(d)	3.13.2(d)	Objective	Identified architectural designs that promote effective information security are employed	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.2(e)	3.13.2(e)	Objective	Identified software development techniques that promote effective information security are employed	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.2(f)	3.13.2(f)	Objective	Identified systems engineering principles that promote effective information security are employed	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.3	3.13.3	Control	Separate user functionality from system management functionality.	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.3(a)	3.13.3(a)	Objective	User functionality is identified	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.3(b)	3.13.3(b)	Objective	System management functionality is identified	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.3(c)	3.13.3(c)	Objective	User functionality is separated from system management functionality	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.4	3.13.4	Control	Prevent unauthorized and unintended information transfer via shared system resources.	Shared
System and Communications Protection (SC)	SC.L2-3.13.4(a)	3.13.4(a)	Objective	Unauthorized and unintended information transfer via shared system resources is prevented.	Shared
System and Communications Protection (SC)	SC.L2-3.13.6	3.13.6	Control	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Shared
System and Communications Protection (SC)	SC.L2-3.13.6(a)	3.13.6(a)	Objective	Network communications traffic is denied by default	Shared
System and Communications Protection (SC)	SC.L2-3.13.6(b)	3.13.6(b)	Objective	Network communications traffic is allowed by exception	Shared
System and Communications Protection (SC)	SC.L2-3.13.7	3.13.7	Control	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.7(a)	3.13.7(a)	Objective	Remote devices are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling).	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.8	3.13.8	Control	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.8(a)	3.13.8(a)	Objective	Cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.8(b)	3.13.8(b)	Objective	Alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.8(c)	3.13.8(c)	Objective	Either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.9	3.13.9	Control	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.9(a)	3.13.9(a)	Objective	A period of inactivity to terminate network connections associated with communications sessions is defined	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.9(b)	3.13.9(b)	Objective	Network connections associated with communications sessions are terminated at the end of the sessions	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.9(c)	3.13.9(c)	Objective	Network connections associated with communications sessions are terminated after the defined period of inactivity	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.10	3.13.10	Control	Establish and manage cryptographic keys for cryptography employed in organizational systems.	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.10(a)	3.13.10(a)	Objective	Cryptographic keys are established whenever cryptography is employed	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.10(b)	3.13.10(b)	Objective	Cryptographic keys are managed whenever cryptography is employed	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.11	3.13.11	Control	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.11(a)	3.13.11(a)	Objective	FIPS-validated cryptography is employed to protect the confidentiality of CUI	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.12	3.13.12	Control	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Customer Responsibility
System and Communications Protection (SC)	SC.L2-3.13.12(a)	3.13.12(a)	Objective	Collaborative computing devices are identified	Customer Responsibility
System and Communications Protection (SC)	SC.L2-3.13.12(b)	3.13.12(b)	Objective	Collaborative computing devices provide indication to users of devices in use	Customer Responsibility
System and Communications Protection (SC)	SC.L2-3.13.12(c)	3.13.12(c)	Objective	Remote activation of collaborative computing devices is prohibited	Customer Responsibility
System and Communications Protection (SC)	SC.L2-3.13.13	3.13.13	Control	Control and monitor the use of mobile code.	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.13(a)	3.13.13(a)	Objective	Use of mobile code is controlled	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.13(b)	3.13.13(b)	Objective	Use of mobile code is monitored	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.14	3.13.14	Control	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	Customer Responsibility
System and Communications Protection (SC)	SC.L2-3.13.14(a)	3.13.14(a)	Objective	Use of Voice over Internet Protocol (VoIP) technologies is controlled	Customer Responsibility
System and Communications Protection (SC)	SC.L2-3.13.14(b)	3.13.14(b)	Objective	Use of Voice over Internet Protocol (VoIP) technologies is monitored.	Customer Responsibility

PreVeil Customer Responsibility Matrix
Controls and Objectives

PREVEIL PROPRIETARY

Assumption: All CUI data will be transmitted and stored using PreVeil, only.

The customer is responsible for determining which controls are applicable, and for developing and maintaining the customer SSP as well as policies, procedures, and supplemental documentation required for compliance related to assessments and audits.

PreVeil claims no responsibility or liability regarding customers information, effort, and execution of their compliance related tasks.

NOTE: The responses contained within this document are specific to PreVeil and the customer's instance of PreVeil. This document does not address any other systems or endpoints that may be considered in scope for a PreVeil customer's assessment.

Control/Objectives Status Legend

Shared	In addition to the customer responsibilities listed in the assumptions and notes statements above, there will be some customer responsibility within the control/objective. This can include, but not limited to, additional documentation, end point management activities, application/system scanning, administrative management activities, asset management, etc. PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way.
PreVeil Inherited	As long as all assumptions and notes above are understood and addressed, PreVeil addresses the control/objective. Note: the customer may still have outstanding responsibilities, based on their internal business processes, technology infrastructure, CUI/FCI handling processes, and/or end point management activities (i.e., ensuring Bitlocker or other hard drive encryption methods are used for any laptop/desktop processing, transmitting, and/or storing CUI). PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information as to how PreVeil manages controls marked in this way for PreVeil customers.
Customer Responsibility	The customer will be reponsible for the objective/control marked "Customer Responsibility". PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way.

Practice Area	CMMC Practice	NIST SP 800-171	Objective/Control	Practice Statement/Objective	Control/Objective Status
System and Communications Protection (SC)	SC.L2-3.13.15	3.13.15	Control	Protect the authenticity of communications sessions.	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.15(a)	3.13.15(a)	Objective	The authenticity of communications sessions is protected.	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.16	3.13.16	Control	Protect the confidentiality of CUI at rest.	PreVeil Inherited
System and Communications Protection (SC)	SC.L2-3.13.16(a)	3.13.16(a)	Objective	The confidentiality of CUI at rest is protected	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.1	3.14.1	Control	Identify, report, and correct information and information system flaws in a timely manner.	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.1(a)	3.14.1(a)	Objective	The time within which to identify system flaws is specified	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.1(b)	3.14.1(b)	Objective	System flaws are identified within the specified time frame	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.1(c)	3.14.1(c)	Objective	The time within which to report system flaws is specified	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.1(d)	3.14.1(d)	Objective	System flaws are reported within the specified time frame	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.1(e)	3.14.1(e)	Objective	The time within which to correct system flaws is specified	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.1(f)	3.14.1(f)	Objective	System flaws are corrected within the specified time frame	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.2	3.14.2	Control	Provide protection from malicious code at appropriate locations within organizational information systems.	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.2(a)	3.14.2(a)	Objective	Designated locations for malicious code protection are identified	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.2(b)	3.14.2(b)	Objective	Protection from malicious code at designated locations is provided	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.4	3.14.4	Control	Update malicious code protection mechanisms when new releases are available.	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.4(a)	3.14.4(a)	Objective	Malicious code protection mechanisms are updated when new releases are available	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.5	3.14.5	Control	Perform periodic scans of the information system and real- time scans of files from external sources as files are downloaded, opened, or executed.	Shared
System and Information Integrity (SI)	SI.L1-3.14.5(a)	3.14.5(a)	Objective	The frequency for malicious code scans is defined	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.5(b)	3.14.5(b)	Objective	Malicious code scans are performed with the defined frequency	PreVeil Inherited
System and Information Integrity (SI)	SI.L1-3.14.5(c)	3.14.5(c)	Objective	Real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed	Shared
System and Information Integrity (SI)	SI.L2-3.14.3	3.14.3	Control	Monitor system security alerts and advisories and take action in response.	Shared
System and Information Integrity (SI)	SI.L2-3.14.3(a)	3.14.3(a)	Objective	Response actions to system security alerts and advisories are identified	Shared
System and Information Integrity (SI)	SI.L2-3.14.3(b)	3.14.3(b)	Objective	System security alerts and advisories are monitored	Shared
System and Information Integrity (SI)	SI.L2-3.14.3(c)	3.14.3(c)	Objective	Actions in response to system security alerts and advisories are taken	Shared
System and Information Integrity (SI)	SI.L2-3.14.6	3.14.6	Control	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Shared
System and Information Integrity (SI)	SI.L2-3.14.6(a)	3.14.6(a)	Objective	The system is monitored to detect attacks and indicators of potential attacks	Shared
System and Information Integrity (SI)	SI.L2-3.14.6(b)	3.14.6(b)	Objective	Inbound communications traffic is monitored to detect attacks and indicators of potential attacks	Shared
System and Information Integrity (SI)	SI.L2-3.14.6(c)	3.14.6(c)	Objective	Outbound communications traffic is monitored to detect attacks and indicators of potential attacks	Shared
System and Information Integrity (SI)	SI.L2-3.14.7	3.14.7	Control	Identify unauthorized use of organizational systems	Shared
System and Information Integrity (SI)	SI.L2-3.14.7(a)	3.14.7(a)	Objective	Authorized use of the system is defined	Shared
System and Information Integrity (SI)	SI.L2-3.14.7(b)	3.14.7(b)	Objective	Unauthorized use of the system is identified	Shared

Total Controls Inherited by PreVeil (PreVeil Inherited)	37
Total Controls supported by PreVeil with Customer Responsibilities (Shared)	65
Total Controls not supported by PreVeil with Customer Responsibilities (Customer Responsibility)	8
Total number of Controls	110

Total Objectives Inherited by PreVeil (PreVeil Inherited)	113
Total Objectives supported by PreVeil with Customer Responsibilities (Shared)	147
Total Objectives not supported by PreVeil with Customer Responsibilities (Customer Responsibility)	60
Total number of Controls	320

Total Controls and Objectives Inherited by PreVeil (PreVeil Inherited)	150
Total Controls and Objectives supported by PreVeil with Customer Responsibilities (Shared)	212
Total Controls and Objectives not supported by PreVeil with Customer Responsibilities (Customer Responsibility)	68
Total number of Controls and Objectives	430