More information: info@kieri.com

Kieri Compliance Documentation (KCD)

What it does…

The KCD is a battle-tested set of policies, procedures, and checklists written in plain English to give you a program for complying with CMMC Level 2 requirements.

These are editable Office documents that, when tailored for your environment and followed, will structure required activities for CMMC compliance and create evidence that each activity was performed on schedule.

Who it's for …

This documentation package provides templates that are easily applicable to enclaves and smaller businesses (1-1,000 users).

The KCD is written to be compatible with any technology solutions, but organizations using Office 365 and Windows 10 will need less customization.

What's included?

- Policies
- Procedures
- User Agreements
- Checklists
- System Security Plan

What's special about these documents?

The KCD is based on the documents Kieri Solutions used to pass their CMMC assessment by the DoD.

The System Security Plan includes example text for common implementations and to reference supporting policies, procedures, and forms from the KCD. More than 240 of the 320 Assessment Objectives of CMMC Level 2 are fully or partially met through the policies and procedures in the KCD.

The KCD is NOT enterprise class. It is designed to be managed by 1-2 people, not a whole team of lawyers, executives, and engineers. The documents are practical, tested, and written in plain English.

Why does the KCD work?

CMMC Level 2 may seem overwhelming, but the trick is to realize that security requirements fall into two categories: **ones that fail if you do nothing** and **ones that stay good if you do nothing**.

The KCD uses a strong **Change Management process** to make sure that you implement new solutions with full security configurations (*controls that stay good if you do nothing*).

The KCD uses a weekly **Cybersecurity Maintenance Checklist** to enforce accountability and remind staff to perform required monitoring, control, and governance over time (*controls that fail if you do nothing*).

Pricing

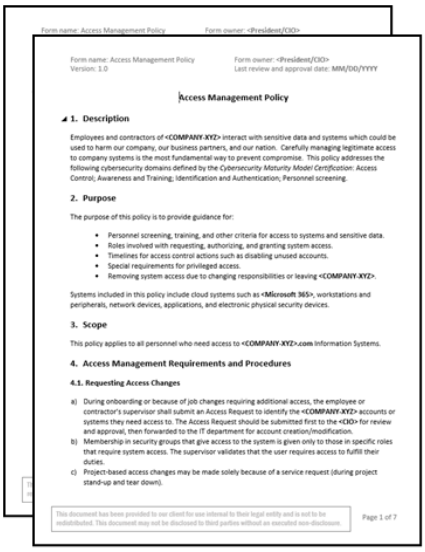
KCD License: $4,700.

Too busy to write documentation?

Ask us about customization services. Our CMMC compliance experts will be happy to work with you to customize the templates for your operational environment. We will explain how to use the compliance documentation and do a quick review and update to get your policies, procedures, and system security plan functional.

25 hours of customization for $6,250

Both processes generate evidence that your organization is performing CMMC Level 2 correctly.



Access Management Policy

1. Description

Employees and contractors of <COMPANY-XYZ> interact with sensitive data and systems which could be used to harm our company, our business partners, and our nation. Carefully managing legitimate access to company systems is the most fundamental way to prevent compromise. This policy addresses the following cybersecurity domains defined by the *Cybersecurity Maturity Model Certification*: Access Control; Awareness and Training; Identification and Authentication; Personnel screening.

2. Purpose

The purpose of this policy is to provide guidance for:

- Personnel screening, training, and other criteria for access to systems and sensitive data.
- Roles involved with requesting, authorizing, and granting system access.
- Timelines for access control actions such as disabling unused accounts.
- Special requirements for privileged access.
- Removing system access due to changing responsibilities or leaving <COMPANY-XYZ>.

Systems included in this policy include cloud systems such as <Microsoft 365>, workstations and peripherals, network devices, applications, and electronic physical security devices.

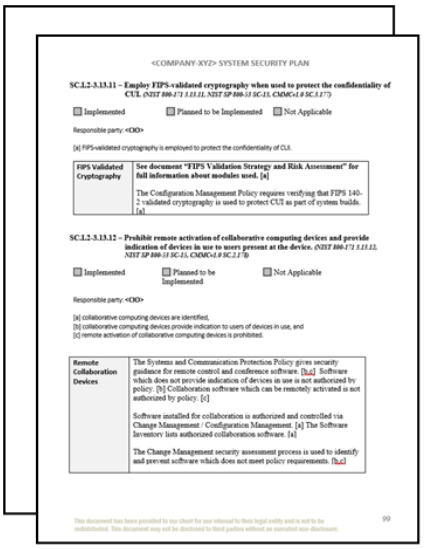
3. Scope

This policy applies to all personnel who need access to <COMPANY-XYZ>.com Information Systems.

4. Access Management Requirements and Procedures

4.1. Requesting Access Changes

a) During onboarding or because of job changes requiring additional access, the employee or contractor's supervisor shall submit an Access Request to identify the <COMPANY-XYZ> accounts or systems they need access to. The Access Request should be submitted first to the <CIO> for review and approval, then forwarded to the IT department for account creation/modification.
b) Membership in security groups that give access to the system is given only to those in specific roles that require system access. The supervisor validates that the user requires access to fulfill their duties.
c) Project-based access changes may be made solely because of a service request (during project stand-up and tear down).



<COMPANY-XYZ> SYSTEM SECURITY PLAN

SC.L2-3.13.11 – Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. *(NIST 800-171 3.13.11, NIST SP 800-53 SC-13, CMMC v1.0 SC.3.177)*

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Responsible party: <CIO>

[a] FIPS-validated cryptography is employed to protect the confidentiality of CUI.

FIPS Validated Cryptography	**See document "FIPS Validation Strategy and Risk Assessment" for full information about modules used. [a]** The Configuration Management Policy requires verifying that FIPS 140-2 validated cryptography is used to protect CUI as part of system builds. [a]

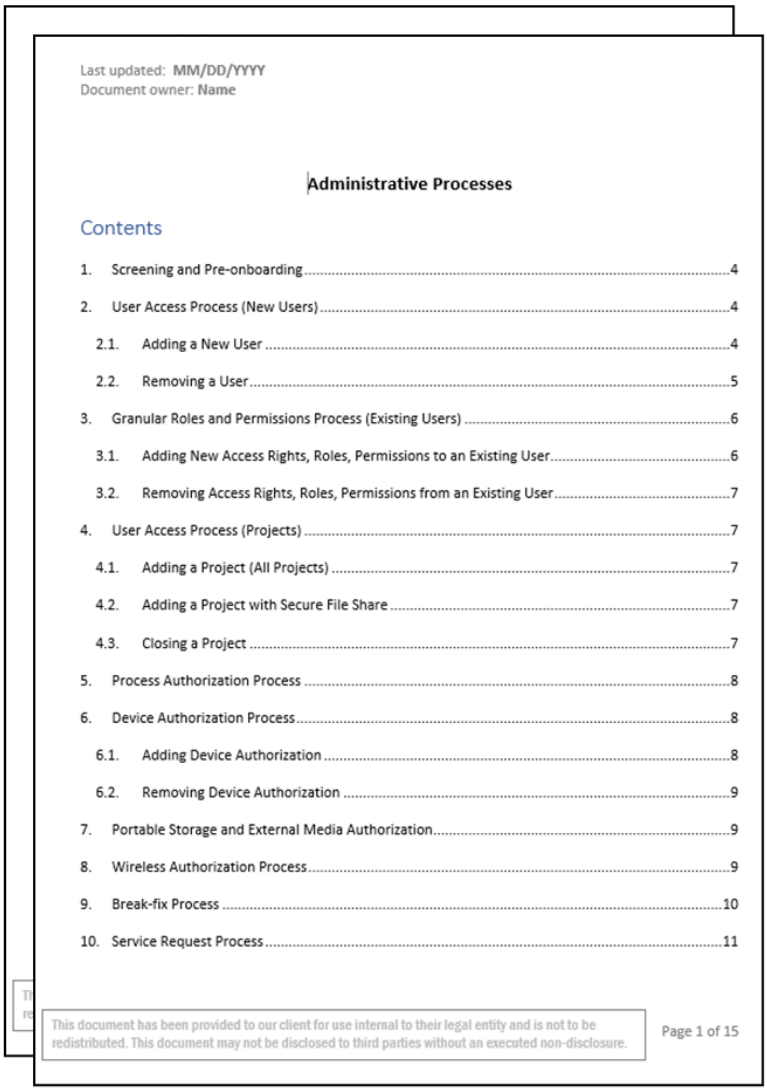
SC.L2-3.13.12 – Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. *(NIST 800-171 3.13.12, NIST SP 800-53 SC-15, CMMC v1.0 SC.3.178)*

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Responsible party: <CIO>

[a] collaborative computing devices are identified,
[b] collaborative computing devices provide indication to users of devices in use, and
[c] remote activation of collaborative computing devices is prohibited.

Remote Collaboration Devices	The Systems and Communication Protection Policy gives security guidance for remote control and conference software. [b,c] Software which does not provide indication of devices in use is not authorized by policy. [b] Collaboration software which can be remotely activated is not authorized by policy. [c] Software installed for collaboration is authorized and controlled via Change Management / Configuration Management. [a] The Software Inventory lists authorized collaboration software. [a] The Change Management security assessment process is used to identify and prevent software which does not meet policy requirements. [b,c]



Last updated: MM/DD/YYYY
Document owner: Name

Administrative Processes

Contents

Frequency	Task	Date	Name	Work Notes (EXAMPLE)
1 Weekly	Review weekly vulnerability summary from threat intelligence (US-CERT). Also describe any bulletins that were of particular concern. Notify affected departments and start service tickets for mitigation as needed.	1/4/2022	Amira	No new high or medium vulnerabilities affecting our information system
2 Monthly (first week of month)	Run a CAB. Make meeting notes per procedure for CAB	1/2/2022	Amira	CAB with CISO and CIO. See CAB Meeting Notes from this day
2 Monthly (first week of month)	Verify operating system is up to date. OS versions can be found in Endpoint mgr > Devices > Monitor > Encryption report.	1/4/2022	Amira	All updated to 10.0.19044.1415
3 Quarterly (first week of Jan, Apr, Jul, Oct)	Test incident response capabilities	12/22/2021	Amira	Performed drill with scenario: "Joe's laptop was stolen." See incident ticket #51 for details
5 Annual (first week Jan)	Review and update all policies and procedures.	12/30/2021	Amira	Reviewed all policies, pushed dates forward
5 Annual (first week Jan)	Perform a full self-assessment of secure.kieri.com controls	2/19/2022	Amira	In progress between 1/15 and 2/19/2022....

How do I find out more?

Contact us at info@kieri.com or check our website at https://kieri.com/kcd

What's Included

Document Name	Description
System Security Plan	Polished system security plan (based on the NIST template) which has extensive instructions and examples pre-written.
Plan of Action	Blank template to be used to create and track your Plan of Action.
FIPS Validation Strategy and Risk Assessment	Partially pre-written document which performs a risk assessment of FIPS vs patching concerns and gives examples of how to describe cryptographic protections for data flows and storage.
Shared Responsibility Matrix	Based on template published by C3PAO Stakeholder Forum. Used by your service provider to delineate responsibilities.

Policies	Description
Access Management Policy	Contains access control procedures specific to accounts (user, privileged, process, shared). Also includes training and screening requirements and identification and authorization requirements.
Audit Management Policy	Defines frequency for audit log reviews, requirements for audit log generation and storage, SIEM. Describes when to start the incident response process.
Change Management Policy	Defines changes which need to go through formal change management and describes how to perform change management.
Configuration Management Policy	Contains required security configurations for all systems, system baselines, data ownership tracking, secure configurations, inventory, least privilege, cryptographic key management, and licensing.
Data Management Policy	Defines different types of data and handling requirements specific to the organization. Gives spillage handling requirements.
Disaster Recovery Policy	Assigns responsibility for creating a disaster recovery plan, defines what should be in it, and describes requirements for safeguarding backups and performing recovery testing.
Facilities Security Policy	Describes facility security systems, physical security measures, logging, and monitoring for facilities.
Incident Management Policy	Defines incidents, describes responsibilities for preparation, drills, recording, response, and reporting.
Risk Assessment Policy	Assigns responsibility and timelines for risk assessment activities such as requirements for threat intelligence monitoring, risk assessments, and ongoing monitoring of controls.
Supply Chain Risk Management Policy	Describes a governance and evaluation program for critical vendors. Not a CMMC requirement, but helpful to have.
Systems and Communication Protection Policy	Describes network security and communications policy to include requirements for remote access, antivirus, gateway security, network access, collaborative computing, remote control, VOIP.
Vulnerability and Patch Management Policy	Contains requirements for performing vulnerability scans, timelines for response to vulnerable systems, legacy systems, and maintenance control.

User Agreements	
Information Systems User Agreement	Acceptable use definition, requirements for passwords and protection of information system.
Issued Equipment Agreement	Instructions to users about issued equipment and required notifications if an incident occurs.
Telework Agreement	General standards for security when working at home.
Protection of Sensitive Information Agreement	In-depth training and instructions for how to handle CUI properly.
Privileged Access Agreement	Acceptable use instructions for privileged users.

Forms and Procedures	
Access Request Form	New user request for access to resources and ensures that the requestor has a work-related need for the resource.
Administrative Processes	Catch-all procedure document which describes how to operate a compliant IT department at a high level.
Audit Log Procedure	Template which can be filled out with steps to perform monitoring according to CMMC.
Disaster Recovery Plan	Not a CMMC requirement. Template which can be used to create a disaster recovery plan with recovery instructions.
Facilities Security – Logbook Template	Used by the front desk to track visitors.
Incident Response Form	Fillable template used to capture required information during cyber incidents.
Incident Response Procedure	Explains how to identify an incident, understand its severity, prioritize it, and investigate and mitigate any attacks/errors, restore operations, and take actions to prevent recurrence.
Personnel Offboarding Checklist	Checklist of activities to perform during offboarding so that all access is removed according to risk.
Publication Review Procedure	Contains steps to ensure that no FCI or CUI is inappropriately published.
Risk Assessment Template	Includes a template with some common risks.
Risk Management Procedure	A procedure for how to identify and determine how to respond to risks.

Repeating Maintenance Activities	
Cybersecurity Maintenance Checklist	Includes both a template as well as examples of completed versions. Used to ensure that scheduled preventative maintenance and compliance tasks are performed.
Change Approvals Board Meeting Notes Template	Includes both a template as well as examples of completed versions. Used to ensure that separation of duties and management governance is performed.
Change Worklog Template	A simple file which can be used to track individual activities during a change ticket.