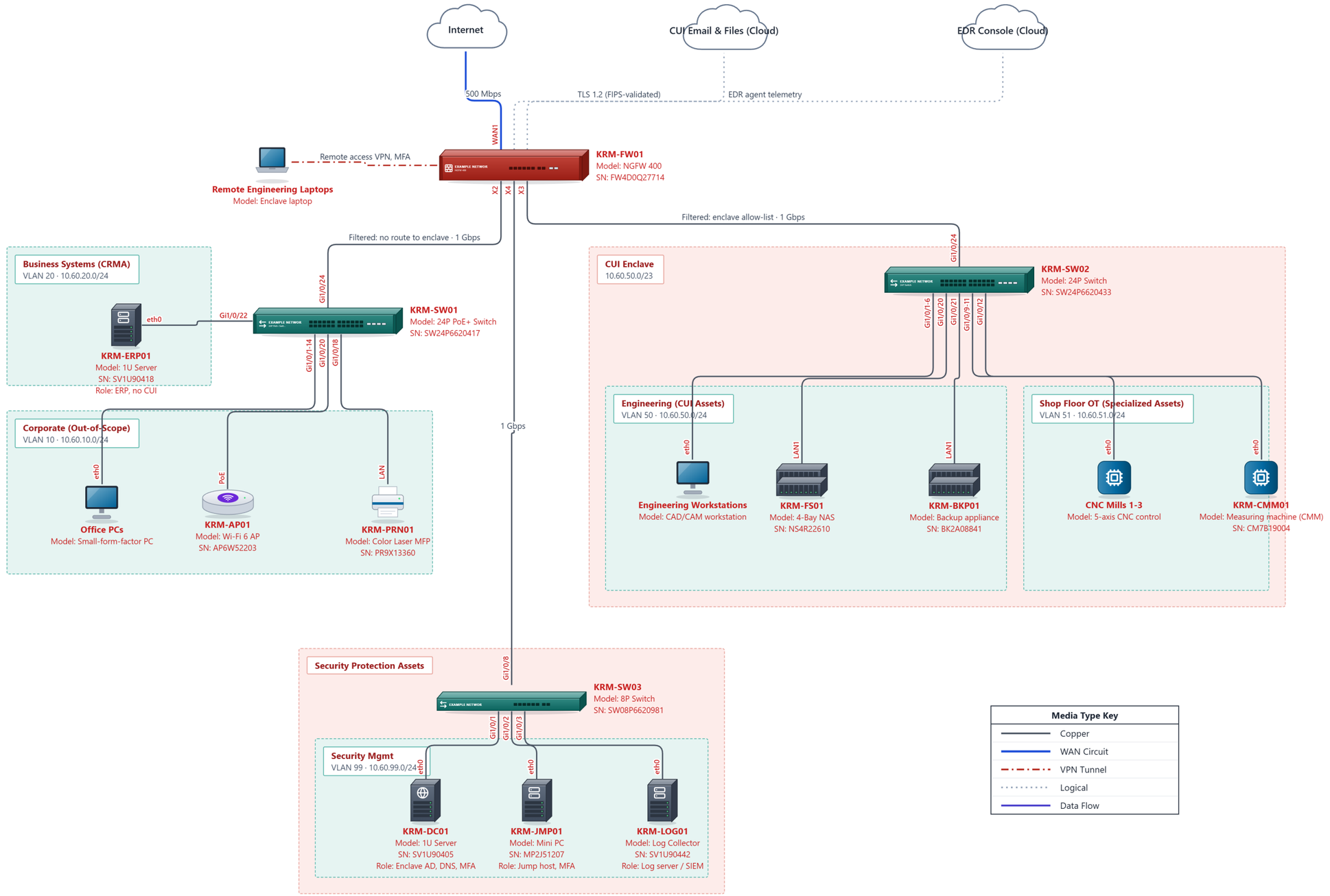
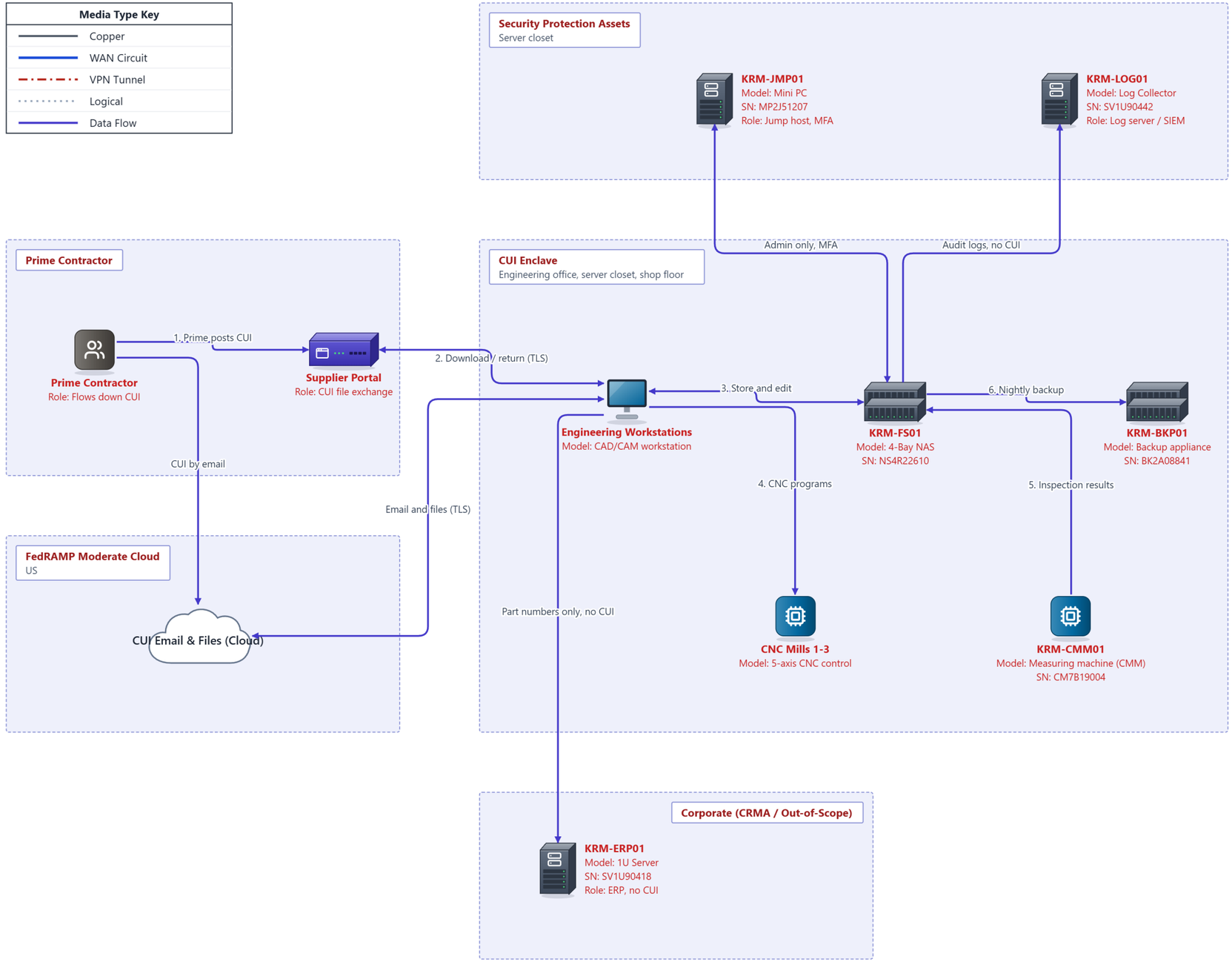


DOCUMENT **CMMC Level 2 - CUI Enclave** Kestrel Ridge Machine Works · 400 Foundry Lane, Springfield	SHEET TITLE **Network**	VERSION 1.0	LAST CHANGED 2026-11-25	VERIFIED
		DRAWN BY	LAST EDITOR	APPROVED

SHEET
1
of 7



DOCUMENT **CMMC Level 2 - CUI Enclave** Kestrel Ridge Machine Works · 400 Foundry Lane, Springfield	SHEET TITLE **CUI Data Flow**	VERSION 1.0	LAST CHANGED 2026-11-25	VERIFIED	SHEET **2** of 7
		DRAWN BY	LAST EDITOR	APPROVED	

Device Inventory 29 devices

Hostname	Type	Vendor / model	Serial	Mgmt IP	Area	Location	Page
Remote Engineering Laptops	Laptop	Example Systems Enclave laptop					Network
Internet	Internet						Network
CUI Email & Files (Cloud)	Cloud Provider						Network
EDR Console (Cloud)	Cloud Provider						Network
KRM-FW01	Firewall	Example Networks NGFW 400	FW4D0Q27714	10.60.99.1		Server closet, Rack 1, U12	Network
KRM-SW01	Switch	Example Networks 24P PoE+ Switch	SW24P6620417	10.60.10.2		Server closet, Rack 1, U10	Network
Office PCs	Workstation	Small-form-factor PC			Corporate (Out-of-Scope)		Network
KRM-AP01	Wireless AP	Example Networks Wi-Fi 6 AP	AP6W52203	10.60.10.40	Corporate (Out-of-Scope)		Network
KRM-PRN01	Printer	Example Imaging Color Laser MFP	PR9X13360	10.60.10.30	Corporate (Out-of-Scope)		Network
KRM-ERP01	Server	Example Systems 1U Server	SV1U90418	10.60.20.10	Business Systems (CRMA)	Server closet, Rack 1, U8	Network
KRM-SW03	Switch	Example Networks 8P Switch	SW08P6620981	10.60.99.3	Security Protection Assets	Server closet, Rack 1, U11	Network
KRM-DC01	DC / DNS / DHCP	Example Systems 1U Server	SV1U90405	10.60.99.10	Security Mgmt	Server closet, Rack 1, U7	Network
KRM-JMP01	Server	Example Systems Mini PC	MP2J51207	10.60.99.20	Security Mgmt	Server closet, shelf	Network
KRM-LOG01	Server	Example Systems Log Collector	SV1U90442	10.60.99.30	Security Mgmt	Server closet, Rack 1, U6	Network
KRM-SW02	Switch	Example Networks 24P Switch	SW24P6620433	10.60.50.2	CUI Enclave	Server closet, Rack 1, U9	Network
Engineering Workstations	Workstation	Example Systems CAD/CAM workstation		10.60.50.21, 10.60.50.22, 10.60.50.23, 10.60.50.24, 10.60.50.25, 10.60.50.26	Engineering (CUI Assets)	Engineering office (badge access)	Network
KRM-FS01	Storage / NAS	Example Storage 4-Bay NAS	NS4R22610	10.60.50.10	Engineering (CUI Assets)	Server closet, Rack 1, U4	Network
KRM-BKP01	Storage / NAS	Example Storage Backup appliance	BK2A08841	10.60.50.11	Engineering (CUI Assets)	Server closet, Rack 1, U2	Network
CNC Mills 1-3	Generic Device	Example Machine Tools 5-axis CNC control		10.60.51.21, 10.60.51.22, 10.60.51.23	Shop Floor OT (Specialized Assets)	Shop floor, cells 1-3	Network
KRM-CMM01	Generic Device	Example Metrology Measuring machine (CMM)	CM7B19004	10.60.51.30	Shop Floor OT (Specialized Assets)	QA lab	Network
CUI Email & Files (Cloud)	Cloud Provider				FedRAMP Moderate Cloud		CUI Data Flow
KRM-JMP01	Server	Example Systems Mini PC	MP2J51207	10.60.99.20	Security Protection Assets	Server closet, shelf	CUI Data Flow
KRM-LOG01	Server	Example Systems Log Collector	SV1U90442	10.60.99.30	Security Protection Assets	Server closet, Rack 1, U6	CUI Data Flow
Engineering Workstations	Workstation	Example Systems CAD/CAM workstation		10.60.50.21, 10.60.50.22, 10.60.50.23, 10.60.50.24, 10.60.50.25, 10.60.50.26	CUI Enclave	Engineering office (badge access)	CUI Data Flow
KRM-FS01	Storage / NAS	Example Storage 4-Bay NAS	NS4R22610	10.60.50.10	CUI Enclave	Server closet, Rack 1, U4	CUI Data Flow
KRM-BKP01	Storage / NAS	Example Storage Backup appliance	BK2A08841	10.60.50.11	CUI Enclave	Server closet, Rack 1, U2	CUI Data Flow
CNC Mills 1-3	Generic Device	Example Machine Tools 5-axis CNC control		10.60.51.21, 10.60.51.22, 10.60.51.23	CUI Enclave	Shop floor, cells 1-3	CUI Data Flow
KRM-CMM01	Generic Device	Example Metrology Measuring machine (CMM)	CM7B19004	10.60.51.30	CUI Enclave	QA lab	CUI Data Flow
KRM-ERP01	Server	Example Systems 1U Server	SV1U90418	10.60.20.10	Corporate (CRMA / Out-of-Scope)	Server closet, Rack 1, U8	CUI Data Flow

Link / Cabling Schedule 19 links

Cable ID	End A	Interface	End B	Interface	Media	Speed	VLANs	Length	Test	Label / notes	Page
	Internet		KRM-FW01	WAN1	WAN Circuit	500 Mbps					Network
	Remote Engineering Laptops		KRM-FW01		VPN Tunnel					Remote access VPN, MFA	Network
	KRM-FW01		CUI Email & Files (Cloud)		Logical					TLS 1.2 (FIPS-validated)	Network
	KRM-FW01		EDR Console (Cloud)		Logical					EDR agent telemetry	Network
KRM-C002	KRM-FW01	X2	KRM-SW01	Gi1/0/24	Copper	1 Gbps	10,20	1 m	Pass	Filtered: no route to enclave	Network
KRM-C004	KRM-FW01	X4	KRM-SW03	Gi1/0/8	Copper	1 Gbps	99	1 m	Pass		Network
KRM-C003	KRM-FW01	X3	KRM-SW02	Gi1/0/24	Copper	1 Gbps	50,51	1 m	Pass	Filtered: enclave allow-list	Network
KRM-D001-014	KRM-SW01	Gi1/0/1-14	Office PCs	eth0	Copper		10		Pass		Network
KRM-D020	KRM-SW01	Gi1/0/20	KRM-AP01	PoE	Copper		10, guest	26 m	Pass		Network
KRM-D018	KRM-SW01	Gi1/0/18	KRM-PRN01	LAN	Copper		10	14 m	Pass		Network
KRM-C010	KRM-SW01	Gi1/0/22	KRM-ERP01	eth0	Copper		20	2 m	Pass		Network
KRM-C020	KRM-SW03	Gi1/0/1	KRM-DC01	eth0	Copper		99	1 m	Pass		Network
KRM-C021	KRM-SW03	Gi1/0/2	KRM-JMP01	eth0	Copper		99	1 m	Pass		Network
KRM-C022	KRM-SW03	Gi1/0/3	KRM-LOG01	eth0	Copper		99	1 m	Pass		Network
KRM-D101-106	KRM-SW02	Gi1/0/1-6	Engineering Workstations	eth0	Copper		50		Pass		Network
KRM-C030	KRM-SW02	Gi1/0/20	KRM-FS01	LAN1	Copper		50	1 m	Pass		Network
KRM-C031	KRM-SW02	Gi1/0/21	KRM-BKP01	LAN1	Copper		50	1 m	Pass		Network
KRM-D201-203	KRM-SW02	Gi1/0/9-11	CNC Mills 1-3	eth0	Copper		51		Pass		Network
KRM-D204	KRM-SW02	Gi1/0/12	KRM-CMM01	eth0	Copper		51	38 m	Pass		Network

VLAN / Subnet Table 5 VLANs

VLAN	Name	Subnet	Gateway	DHCP scope / helper	Devices	Page
10	Corporate (Out-of-Scope)	10.60.10.0/24	10.60.10.1	KRM-FW01	3	Network
20	Business Systems (CRMA)	10.60.20.0/24	10.60.20.1	Static	1	Network
50	Engineering (CUI Assets)	10.60.50.0/24	10.60.50.1	Static	3	Network
51	Shop Floor OT (Specialized Assets)	10.60.51.0/24	10.60.51.1	Static	2	Network
99	Security Mgmt	10.60.99.0/24	10.60.99.1	Static	3	Network

Data Flows 11 flows

From	To	Data	Class.	Sensitive data	Protocol / port	Encryption	Purpose	Page
Prime Contractor (Prime Contractor)	Supplier Portal (Prime Contractor)	Drawings, specs, POs	Restricted	CUI	HTTPS 443	TLS 1.2	Flow down technical data for the order	CUI Data Flow
Supplier Portal (Prime Contractor)	Engineering Workstations (CUI Enclave)	Drawings in; inspection reports out	Restricted	CUI	HTTPS 443	TLS 1.2	Get CUI into the enclave and deliver results back to the prime	CUI Data Flow
Prime Contractor (Prime Contractor)	CUI Email & Files (Cloud) (FedRAMP Moderate Cloud)	Email with CUI attachments	Restricted	CUI	SMTP TLS 25	TLS 1.2	Questions and revisions from the prime	CUI Data Flow
CUI Email & Files (Cloud) (FedRAMP Moderate Cloud)	Engineering Workstations (CUI Enclave)	CUI email and shared files	Restricted	CUI	HTTPS 443	TLS 1.2	CUI email, reachable only from enclave devices	CUI Data Flow
Engineering Workstations (CUI Enclave)	KRM-FS01 (CUI Enclave)	Drawings, CAM programs	Restricted	CUI	SMB 3.1.1 (encrypted)	Other encryption	Engineering work on CUI	CUI Data Flow
Engineering Workstations (CUI Enclave)	CNC Mills 1-3 (CUI Enclave)	G-code from CUI drawings	Restricted	CUI	DNC over SMB	Other encryption	Machine the parts	CUI Data Flow
KRM-CMM01 (CUI Enclave)	KRM-FS01 (CUI Enclave)	Inspection reports	Restricted	CUI	SMB 3.1.1 (encrypted)	Other encryption	Quality records for the prime	CUI Data Flow
KRM-FS01 (CUI Enclave)	KRM-BKP01 (CUI Enclave)	File server backup	Restricted	CUI	Backup agent 10000	TLS 1.2	Recover CUI after loss or ransomware	CUI Data Flow
Engineering Workstations (CUI Enclave)	KRM-ERP01 (Corporate (CRMA / Out-of-Scope))	Part numbers, quantities, ship dates	Internal		HTTPS 443	TLS 1.2	Order and shipping records	CUI Data Flow
KRM-JMP01 (Security Protection Assets)	KRM-FS01 (CUI Enclave)	Admin sessions	Confidential		RDP 3389	TLS 1.2	Administration through the jump host	CUI Data Flow
KRM-FS01 (CUI Enclave)	KRM-LOG01 (Security Protection Assets)	Audit logs	Internal		Syslog 6514	TLS 1.2	Logging and monitoring	CUI Data Flow

Data Stores 4 stores

Data store	Stores	Class.	Sensitive data	Encrypted at rest	Kept for	Region	Owner	Boundary
KRM-FS01	Drawings, specs, CAM programs, inspection reports	Restricted	CUI	Yes	Per contract, then destroyed	Server closet, Rack 1	Engineering	
KRM-BKP01	Nightly backups of KRM-FS01; weekly encrypted copy rotated to an offsite safe	Restricted	CUI	Yes	30 daily, 12 monthly	Server closet, Rack 1; offsite safe	IT	
KRM-FS01	Drawings, specs, CAM programs, inspection reports	Restricted	CUI	Yes	Per contract, then destroyed	Server closet, Rack 1	Engineering	CUI Enclave
KRM-BKP01	Nightly backups of KRM-FS01; weekly encrypted copy rotated to an offsite safe	Restricted	CUI	Yes	30 daily, 12 monthly	Server closet, Rack 1; offsite safe	IT	CUI Enclave