FUTUREFEED

Control-Level Responsibility Matrix

This matrix documents the division of responsibilities between FutureFeed and its customers under CMMC 2.0 / 32 CFR Part 170. It is provided as a customer convenience tool; a formal CRM is not a regulatory requirement for Contractor Risk Managed Assets (CRMAs). *Rev. April 2026*

RECOMMENDED ASSET CLASSIFICATION: CONTRACTOR RISK MANAGED ASSET (CRMA)

FutureFeed is a GRC platform hosted in AWS GovCloud (US) with achieved FedRAMP Moderate Equivalency. It is not a CUI asset and does not perform technical security enforcement within a customer's CUI boundary. Customers must document this CRMA classification within their own System Security Plan (SSP). Treating FutureFeed as out-of-scope is a common and avoidable scoping error — assessors routinely review GRC platforms.

OWNERSHIP KEY **FutureFeed** = Platform-managed **Customer** = Customer action required **Shared** = Joint responsibility **Policy** = Organizational policy

CONTROL / RESPONSIBILITY AREA	OWNER	DESCRIPTION	NOTES / CUSTOMER ACTIONS
PLATFORM & INFRASTRUCTURE SECURITY			
Secure Hosting Environment *AC / SC*	FutureFeed	FutureFeed operates entirely within AWS GovCloud (US), managed by Project Hosts. Infrastructure-level security controls — including physical security, availability, and boundary protection — are the exclusive responsibility of FutureFeed and its hosting partners.	*No customer action required. FedRAMP Moderate Equivalency documentation is available upon request.*
Data Encryption (Transit & Rest) *SC-8 / SC-28*	FutureFeed	All data transmitted to and stored within FutureFeed is encrypted using industry-standard protocols. Encryption key management and cipher configuration are managed by FutureFeed.	*Customers should ensure local endpoints and browsers support modern TLS configurations.*
Platform Logging & Monitoring *AU-2 / AU-12 / SI-4*	FutureFeed	FutureFeed is responsible for logging, monitoring, and maintaining platform integrity, including audit logs of system events and platform-level anomaly detection.	*FutureFeed does NOT provide security monitoring within a customer's CUI boundary. Customers must maintain independent SIEM/logging for their own environments.*
Application Security & Patch Management *SI-2 / SA-11*	FutureFeed	FutureFeed manages application-layer security including vulnerability management, patch deployment, and secure development practices for the FutureFeed platform itself.	*Customers are responsible for patching their own endpoints, browsers, and network infrastructure used to access the platform.*

CONTROL / RESPONSIBILITY AREA	OWNER	DESCRIPTION	NOTES / CUSTOMER ACTIONS
System Availability & Business Continuity *CP-9 / CP-10*	**FutureFeed**	FutureFeed maintains backup, recovery, and business continuity processes for the platform and all customer data stored within it.	*Customers should maintain local copies of critical SSP artifacts to support their own compliance program continuity independent of platform availability.*
IDENTITY & ACCESS MANAGEMENT			
Application-Level Access Controls *AC-2 / AC-3*	**FutureFeed**	FutureFeed provides and enforces role-based access controls within the platform, defining permitted actions and accessible data for each role at the application layer.	*Customers must assign roles appropriately and review permissions regularly to maintain the principle of least privilege.*
Multi-Factor Authentication Enforcement *IA-2(1) / IA-2(2)*	**FutureFeed**	FutureFeed enforces MFA for all user access to the platform. MFA cannot be bypassed or disabled by users or customer administrators.	*Customers must ensure all users complete MFA enrollment. Loss of MFA access must be reported to FutureFeed support promptly.*
User Account Lifecycle Management *AC-2 / PS-4 / PS-5*	**Customer**	Customers are solely responsible for managing user account lifecycles within their FutureFeed tenant — provisioning new users, modifying roles, and promptly deprovisioning accounts upon personnel departure or role change.	*ACTION REQUIRED: Establish a formal onboarding/offboarding process. Document periodic access reviews in the customer's SSP. FutureFeed provides the opportunity to configure time-limited access for users with temporary needs.*
Periodic Access Review *AC-2(j) / CA-7*	**Customer**	Customers must periodically review all user accounts and permissions within FutureFeed to verify access remains appropriate and no unauthorized or stale accounts exist.	*ACTION REQUIRED: Document review frequency, methodology, and results. CMMC assessors may request evidence of completed access reviews.*
DATA GOVERNANCE & CUI BOUNDARY INTEGRITY			
CUI Non-Introduction Policy *AC / CM / MP*	**Policy**	Customers must maintain and enforce an organizational policy explicitly prohibiting the intentional upload or storage of CUI within FutureFeed. FutureFeed is a governance and documentation platform — not an authorized CUI repository.	*ACTION REQUIRED: Formalize in writing; reference in SSP; brief all FutureFeed users on this restriction prior to granting access.*
Inadvertent CUI Spill Response *IR-4 / MP-6*	**Shared**	If CUI is inadvertently introduced, the customer bears responsibility for detecting the spill and initiating incident response. FutureFeed is capable of securely containing	*Include FutureFeed in incident response runbooks as a potential spill surface. Notify FutureFeed support immediately upon confirmed or suspected CUI introduction.*

<table>
<tr><th>CONTROL / RESPONSIBILITY AREA</th><th>OWNER</th><th>DESCRIPTION</th><th>NOTES / CUSTOMER ACTIONS</th></tr>
<tr><td></td><td></td><td>CUI if introduced, but is neither designed nor scoped as a CUI system.</td><td></td></tr>
<tr><td>Content & Artifact Review
CM-12 / MP-3</td><td>Customer</td><td>Customers are responsible for reviewing all content and evidence artifacts uploaded to FutureFeed to ensure they do not contain CUI, export-controlled data, or information exceeding the platform's authorized data classification.</td><td>ACTION REQUIRED: Implement a pre-upload review step in internal workflows. Sensitive artifacts (SSPs, POA&Ms, architecture docs) — while not CUI — must be access-controlled appropriately.</td></tr>
<tr><td>Sensitive Security Documentation Handling
AC / MP</td><td>Customer</td><td>FutureFeed stores inherently sensitive security information including control implementations, network references, vulnerability data, and POA&Ms. While not CUI, unauthorized disclosure could increase risk to the customer's CUI environment.</td><td>Assign roles deliberately using FutureFeed's four available user roles:<table><tr><th>Role</th><th>Appropriate For</th></tr><tr><td>No Access</td><td>Personnel who no longer need platform access; use promptly on departure or role change</td></tr><tr><td>Standard</td><td>Active compliance staff who contribute to SSP content and evidence</td></tr><tr><td>Admin</td><td>Limited to personnel with a direct need to configure the tenant; minimize this count</td></tr><tr><td>Assessor (read-only)</td><td>C3PAO assessors and internal auditors only; prevents modification of documentation</td></tr></table>Periodically audit user role assignments and deprovision or downgrade anyone whose responsibilities no longer require access. Document reviews in your SSP.
Note: FutureFeed does not provide field-level or document-level access restrictions within a role — role assignment is your primary access control lever.</td></tr>
<tr><td colspan="4">CMMC SCOPING & COMPLIANCE DOCUMENTATION</td></tr>
<tr><td>CRMA Classification & SSP Documentation</td><td>Customer</td><td>Customers are responsible for formally documenting FutureFeed's classification as a Contractor Risk</td><td>ACTION REQUIRED: Do not treat FutureFeed as out-of-scope. Reference FutureFeed's FedRAMP</td></tr>
</table>

CONTROL / RESPONSIBILITY AREA	OWNER	DESCRIPTION	NOTES / CUSTOMER ACTIONS
CA-2 / PL-2		Managed Asset (CRMA) in their own SSP, including the rationale for that classification and how associated risks are managed.	*Moderate Equivalency as part of the CRMA risk justification.*
Vendor Risk Management & Due Diligence *SA-9 / SR-3*	**Shared**	FutureFeed maintains vendor security documentation and posture evidence (including FedRAMP Moderate Equivalency). Customers are responsible for conducting and documenting their vendor risk review as part of their supply chain risk management process.	*Download and follow FutureFeed's CRM to demonstrate fulfillment of vendor risk management assessment requirements.*
Contractual Security Protections *SA-9 / AT*	**FutureFeed**	FutureFeed maintains contractual confidentiality and security obligations with customers and establishes equivalent protections with subservice providers. These contractual controls support the CRMA classification risk framework.	*Retain the FutureFeed service agreement as vendor documentation. Its security terms are relevant to assessor inquiries.*
OPERATIONAL GOVERNANCE & TRAINING			
Acceptable Use & Internal Policy Alignment *PL / PS*	**Customer**	Customers are responsible for operating FutureFeed in accordance with their internal security and acceptable use policies, and ensuring its use is consistent with their broader CMMC compliance posture.	*ACTION REQUIRED: Reference FutureFeed explicitly in internal acceptable use policies and system inventories. Inform users of restrictions before granting access.*
User Awareness & Training *AT-2 / AT-3*	**Customer**	Customers are responsible for ensuring all FutureFeed users receive appropriate cybersecurity awareness training, including training on the prohibition against uploading CUI to the platform.	*ACTION REQUIRED: Document FutureFeed-specific restrictions in your internal training materials. Maintain training completion records as CMMC assessment evidence.*
Incident Reporting to FutureFeed *IR-6 / IR-7*	**Shared**	FutureFeed monitors the platform and notifies customers of security events affecting the FutureFeed environment. Customers must report suspected security incidents, unauthorized access, or data integrity concerns within their FutureFeed tenant to FutureFeed support promptly. Real-time platform status and incident notifications are available at futurefeed.statuspage.io.	*Contact: support@futurefeed.co or 1-844-725-8252. Include FutureFeed in customer incident response procedures as both a potential incident surface and a notification recipient.*

Intended Use and CUI Boundaries

- **Intended Use**: FutureFeed is designed to store the documentation and evidence used to build, manage, and demonstrate your security program, including network diagrams, system configurations, policies, procedures, and implementation statements mapped to controls.
- **CUI Deliverables**: FutureFeed is not intended to be the system of record or primary repository for CUI that exists as a government or contract deliverable, such as Controlled Technical Information (CTI), export-controlled data, or other CUI-bearing deliverables produced for or transmitted to a prime contractor or the Government. Those materials should be maintained in systems specifically intended and authorized for that purpose.
- **FutureFeed's Role**: FutureFeed operates in a FedRAMP Moderate-equivalent environment on AWS GovCloud. It is not intended to function as your authorized CUI enclave. Customers remain responsible for identifying CUI and determining the appropriate system of record for that information.
- **Scoping**: We recommend documenting FutureFeed in your SSP as a Contractor Risk Managed Asset (CRMA)—an asset that can, but is not intended to, store CUI. Final asset categorization should be determined between the customer and their assessor.
- **Access**: Use individual user accounts and keep multi-factor authentication enabled. User credentials should not be shared.
- **Security Functions**: FutureFeed is intended to document and track security activities, including monitoring, logging, enforcement, and incident response. Organizations should continue using purpose-built tools to perform those functions.

Important Scoping Note for CMMC Assessments

> FutureFeed's intended function is governance, risk management, and compliance documentation. It records and describes an organization's security program rather than hosting CUI or directly enforcing security controls. Under CMMC 2.0 (32 CFR Part 170), asset categorization is based on intended function, which is why we view FutureFeed as a CRMA rather than a Security Protection Asset (SPA). A Customer Responsibility Matrix is not a regulatory requirement for CRMAs; we provide one as a convenience to help reduce assessment friction. Customers may also reference FutureFeed's independently audited FedRAMP Moderate Equivalency, validated by Lunarline, as part of their risk determination.