

SYSTEM ACCESS REQUEST

Type of Request: <input type="checkbox"/> Initial <input type="checkbox"/> Modification <input type="checkbox"/> Deactivate <input type="checkbox"/> Active	Date (DDMMYYYY)	System Name: Armis FedRAMP Edition
---	------------------------	--

PART 1: USER INFORMATION (To be completed by Requestor)

1. Name (Last, First, Middle Initial)		2. Organization	3. Office/Department
4. Phone	5. Official E-Mail Address		6. Job Title and Grade/Rank
7. Official Mailing Address		8. Citizenship: <input type="checkbox"/> US <input type="checkbox"/> Foreign National <input type="checkbox"/> Other	9. Designation: <input type="checkbox"/> Civilian <input type="checkbox"/> Contractor
10. IA Training/Cyber Awareness Date Completed (DDMMYYYY)	11. User Signature		12. Date (DDMMYYYY)

PART II: ARMIS ISSO APPROVAL

13. Justification for Access: <input type="checkbox"/> Federal <input type="checkbox"/> Industry Partner		14. Type of Access Required: <input type="checkbox"/> Viewer <input type="checkbox"/> Editor
15. Armis ISSO (Name, Email, Phone, Organization)		
16. Armis ISSO Signature		17. Date (DDMMYYYY)

PART III: ARMIS' SYSTEM ADMINISTRATOR/STAFF ACTION

User ID Assigned		Folder Access Given
Date Processed (DDMMYYYY)	Processed By (Signature)	Revalidation Date (DDMMYYYY)

Language for AFE/AGC Access Form
SYSTEM Name: Armis FedRAMP Edition (AFE) / Armis Government Cloud (AGC)

System Name: Armis FedRAMP Edition (AFE) Authority and Scope

In accordance with Part I, Block 11, all external users granted access to the Armis FedRAMP Edition (AFE) must acknowledge these Rules of Behavior (RoB). This document serves as a formal artifact to enable independent assessment and verification of security compliance.

1. User Attestation

As the individuals identified in Part I, Block 1 (Name), I acknowledge that I am being granted privileges to a SharePoint Portal managed by Armis. I agree to the following mandates:

- Security Baseline: I shall strictly adhere to the FedRAMP security controls baseline assigned to this Cloud Service Offering (CSO).
- Operational Principles: I shall abide by the principles of Separation of Duties and Least Privilege at all times.
- System Integrity: I will only access files in AFE SharePoint on a system that has been approved by my organization
- Official Business: I will process only data pertaining to official business and authorized for this system in my capacity as user.
- Authentication: I shall use only the designated multi-factor authentication (MFA) method for administrative components. I will not attempt to access this administrative role using standard internal user credentials.

2. Privacy Statement

When you access the AFE SharePoint environment via your organization's Identity Provider (IdP), we collect and process certain personal data necessary to facilitate secure access and collaboration. This data is generally provided by your IdP during the "handshake" (authentication) process and includes:

- Identity Data: Full name, professional email address, and unique user identifier (UPN/Object ID).
- Technical Log Data: IP address, browser type, device information, and timestamps of access.
- Activity Data: A record of files accessed, edited, or downloaded, and any communications (comments/chats) made within the environment.

We process this data for the following purposes:

- Security and Authentication: To verify your identity and ensure only authorized personnel access our proprietary data.
- Audit and Compliance: To maintain legally required audit logs of who accessed what information and when.
- Collaboration: To allow the Armis team members to identify you and collaborate with you effectively on shared documents.

3. Protection of Information and Assets

- Data Safeguarding: I will safeguard all resources against waste, loss, abuse, and misappropriation, ensuring the Confidentiality, Integrity, and Availability (CIA) of federal data.
- Legal Compliance: I shall comply with all copyright, site licenses, Privacy Act, and Supply Chain requirements.
- Records Management: Official records (electronic and hardcopy) will be stored and disposed of per CSP policies and standards.

4. Reporting and Maintenance

- Incident Response: I will follow established protocols for reporting security incidents to superiors in accordance with the Armis Incident Response Procedures and FedRAMP Communications Procedures.
- Training and Certification: In alignment with Part I, Block 10, I will maintain all required professional certifications and regularly attend computer security awareness and privacy training.

5. Mission Owner Identity Provisioning Responsibilities

Mission Owner is required to configure their Identity Provider (IdP) to authenticate against the AFE SharePoint tenant.

6. Acknowledgement and Liability

By my digital signature as required in Part I, Block 11, I verify that I have read and understand these rules. I acknowledge that obtaining information in violation of these restrictions may constitute a violation of the Computer Fraud and Abuse Act and result in the immediate deactivation.

User Signature	Date (DDMMYYYY)