SYSTEM ACCESS REQUEST

Type of Request:	**Date** (DDMMMYYYY)	**System Name:**
☐Initial ☐Modification ☐Deactivate ☐Active		Armis FedRAMP

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 Adress		**8. Citizenship:** ☐US ☐Foreign National ☐Other	**9. Designation:** ☐Civilian ☐Contractor
10. IA Training/Cyber Awareness Date Completed (DDMMYYYY)		**11. User Signature**	**12. Date** (DDMMMYYYY)

PART II: ARMIS ISSO APPROVAL

13. Justification for Access: ☐Federal ☐Industry Partner	**14. Type of Access Required:** ☐Viewer ☐Editor
15. Armis ISSO (Name, Email, Phone, Organization)	
16. Armis ISSO Signature	**17. Date** (DDMMYYYY)

PART IV: 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)

1. Authority and Scope

In accordance with Part II, Block 13 (Justification), all external users granted access to the Armis FedRAMP Edition (AFE) or Armis Government Cloud (AGC) must acknowledge these Rules of Behavior (RoB). This document serves as a formal artifact to enable independent assessment and verification of security compliance.

2. 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/AGC 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.

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. Acknowledgement and Liability

By my signature (digital or physical) 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.

FINAL ACKNOWLEDGEMENT	
User Signature	**Date** (DDMMYYYY)