Plan of Action and Milestones (POA&M) – Cloud-Based HRMS

This POA&M documents corrective actions for security control weaknesses identified during the security assessment of the Cloud-Based HRMS system hosted on AWS.

Weakness ID	Description	Control(s) Affected	Planned Corrective Action	Milestones	Resources Required	Scheduled Completion Date	Status
POAM-001	Orphaned IAM accounts not disabled after staff offboarding	AC-2	Implement automated de-provisioning via AWS SSO lifecycle policies and HRMS-IT workflow integration	Design -> Implement automation -> Test -> Deploy	IAM Admin, HRMS Admin	2025-09-15	Open
POAM-002	Certain HR and payroll roles have overlapping permissions	AC-5	Review and update IAM role definitions to enforce separation of duties	Access review -> Role redesign -> Apply IAM policy updates -> Verify	Security Engineer, HR Lead	2025-09-30	Open
POAM-003	IAM policies using wildcards granting excessive privileges	AC-6	Apply least privilege by using explicit resource ARNs and scoped permissions	Policy audit -> Remove wildcards -> Test access -> Approve changes	IAM Admin, Security Engineer	2025-08-31	In Progress
POAM-004	Account lockout thresholds not enforced in HRMS application	AC-7	Configure application authentication settings to lock accounts after 5 failed attempts	Config update -> Test -> Deploy -> Monitor	App Dev Team, Security Engineer	2025-09-10	Open
POAM-005	Audit logs missing IP	AU-3	Update logging	Log config	App Dev Team	2025-08-25	In Progres

	address field for certain user activities		configuration to include full contextual metadata	update -> Test logs -> Deploy to prod			s
POAM-006	No formal monthly log review process	AU-6	Establish a documented monthly log review SOP and assign log review owners	Draft SOP -> Train staff -> Implement review schedule	SOC Analyst, Security Manager	2025-09-20	Open
POAM-007	Audit logs stored in S3 without bucket policy restrictions	AU-9	Apply restrictive S3 bucket policies and enable server-side encryption	Policy design -> Apply restrictions -> Test access	S3 Admin, Security Engineer	2025-08-20	In Progress
POAM-008	Privileged admin actions not tied to named identities	AU-10	Implement individual IAM user accounts for all admins with MFA enforced	Account setup -> Enforce MFA -> Remove shared creds	IAM Admin, Security Engineer	2025-09-05	Open
POAM-009	No formal privacy awareness training for HR staff	AT-2	Develop and roll out privacy training covering PII handling	Create training material -> Deliver sessions -> Track attendance	Privacy Officer, HR Lead	2025-09-25	Planned
POAM-010	No role-specific security training for developers	AT-3	Implement secure coding training tailored to HRMS developers	Select course -> Deliver -> Assess knowledge retention	Security Manager, Dev Lead	2025-10-10	Planned
POAM-011	Risk assessment not updated in last 12 months	RA-3	Conduct updated risk assessment incorporating latest threats	Plan -> Assess -> Document -> Approve	Risk Officer, Security Manager	2025-09-30	Open
POAM-012	No vulnerability scans on	RA-5	Integrate Lambda scanning via	Tool selection ->	DevOps, Security Engineer	2025-09-18	Open

	AWS Lambda functions		AWS CodePipeline security scans	Integrate scans -> Test -> Deploy			
POAM-013	Delayed patching of non-critical servers beyond policy timelines	SI-2	Enforce patch timelines with AWS Systems Manager Patch Manager automation	Configure patch rules -> Test -> Deploy	Systems Admin	2025-09-08	In Progress
POAM-014	GuardDuty alerts not integrated into centralized SIEM	SI-4	Integrate GuardDuty with AWS OpenSearch or third-party SIEM for real-time alerts	Design -> Connect feeds -> Test -> Deploy	SOC Analyst, Security Engineer	2025-09-28	Open