BELINA TIME SYSTEMS (PRIVATE) LIMITED

Belina Payroll AWS Security Architecture

Executive Summary and Architectural Vision

The Belina Payroll System processes highly sensitive Personally Identifiable Information (PII) and financial data. This architecture is designed around an existing, highly isolated private network model, with access restricted exclusively to authorized Belina users via AWS Identity centre, SCP, IAM roles/Policies and defined ingress points. The architecture is guided by a robust, existing framework of ISO-certified policies (including Cloud Security, Access Control, Password, Acceptable Use, and Data Protection/Privacy).

The design maintains a Defense-in-Depth posture ensuring compliance with local and international standards (e.g. ISO27001 and CDPA).

Core Security Principles

1. The core application and data servers have zero direct access to the public internet (Egress Control enforced).
2. Access is only permitted from designated IP addresses and is secured via a managed ingress solution.
3. All architectural decisions must align with the current ISO-certified policy framework.
4. Mandatory Data Protection: All PII and financial data must be encrypted at rest and in transit.

Future State Architecture Design

The target architecture is built on the AWS Security Reference Architecture (SRA) multi-account model, emphasizing internal segmentation for the front end, backend and database and tenant Isolation achieved at Database level

Foundational Layer: AWS Organization and Accounts

We will continue to use AWS Organizations to enforce security policies at the organizational level using Service Control Policies (SCPs).

Account Name	Purpose	Key Services
Management	Centralized billing, organization root. Access is highly restricted.	AWS Organizations, Billing
Security	Centralized security tooling, read-only audit access.	AWS Security Hub, GuardDuty, Audit Logs (S3/CloudWatch), AWS IAM Identity Center (SSO)

Logging	Centralized, immutable repository for all logs (VPC Flow, CloudTrail, application).	Amazon S3 (WORM/Vault Lock), AWS CloudTrail, AWS Backup Vaults
Production	Hosts production environments	VPC, EC2, RDS, KMS,WAF Auto
Development/QA/Pre-production	Hosts non-production environments. No real PII data permitted.	VPC, EC2, RDS, KMS,WAF Auto

Identity and Access Management (IAM)

Identity is the primary control point in this architecture, governing access to WorkSpaces and the underlying servers.

Network and Perimeter Protection - Isolation Focus

The architecture follows AWS best practices and reduces is entirely private, eliminating external attack surface points (Public IPs, Load Balancers, WAF).

Control Area	Requirement	AWS Solution
Network Segmentation	Strict separation of the WorkSpaces layer from the application/database layers.	VPC with Private Subnets for WorkSpaces, all layers communicate using Private IP only.
Egress Control	The servers have NO access to the internet. All outbound application traffic must be blocked.	Strict Network ACLs (NACLs) on all Private Subnets to deny 0.0.0.0/0 (internet) traffic. Use VPC Gateway Endpoints for secure, private access to AWS services
Traffic Inspection	Continuous monitoring for unauthorized internal traffic (lateral movement).	VPC Flow Logs enabled on all subnets, centrally monitored in the Logging Account for policy compliance.

Data Protection (PII and Financial Data)

Control Area	Requirement	AWS Solution
Encryption at Rest	All PII data (employee names, bank accounts, IDs) must be encrypted.	AWS Key Management Service (KMS).
Encryption in Transit	Encrypt all communication channels, even within the private VPC.	Enforce TLS 1.2+ and Traffic moves using private links.

Backup and Recovery Integrity	Ensure secure, immutable backups that align with ISO retention policies.	AWS Backup and Snapshots

Detection and Monitoring

All detection and monitoring must focus on identifying internal anomalies, lateral movement, and compliance drift in the isolated environment.

Control Area	Requirement	AWS Solution
Continuous Threat Detection	Automated monitoring for suspicious internal activity, credential compromise, and unauthorized port activity within the VPC.	Amazon GuardDuty
Vulnerability Scanning	Identify misconfigurations and vulnerabilities in infrastructure and WorkSpace images.	Amazon Inspector for scanning EC2 instances and lambdas
Compliance Assurance	Ensure continuous alignment with ISO and internal access control policies.	AWS Config enabled to monitor compliance against established baseline rules (e.g., ensuring no internet gateways are attached to Production VPCs, mandatory KMS encryption is active).