OUTSTANDING ARTIFACTS/EVIDENCES

Following our review of the submitted materials for the Infrastructure & Security QA assessment, we would like to thank you for the comprehensive documentation already provided. The current artifacts have enabled a strong initial evaluation across architecture, security, and core platform configuration. However, to complete an evidence-based assessment in line with the stated requirements, there are several items for which supporting documentation or evidence that are still outstanding or only partially provided. We kindly request that you provide the following additional artifacts or evidence where available:

1. ENVIRONMENT & DEPLOYMENT

- Documentation of environment separation (development, staging, production)
- CI/CD pipeline configurations (e.g., GitHub Actions, Azure DevOps)
- Evidence of deployment workflows (pipeline runs, logs, approvals)
- Deployment strategy (e.g., rolling, blue-green, canary)
- Rollback procedures and release management controls

2. INFRASTRUCTURE AS CODE

- Declarative Infrastructure as Code (Terraform, Bicep, or ARM templates)
- Evidence of drift control and environment consistency

3. DATA LAYER & RESILIENCE

- Database sizing rationale and performance considerations
- Documented failover procedures for PostgreSQL and Redis
- Plan for a failover or recovery testing
- Redis high availability or clustering strategy (if applicable)

4. NETWORKING & SECURITY

- Detailed NSG rules and firewall configurations (rule-level evidence)
- Cloudflare/WAF configuration details (e.g., rate limiting, bot protection rules)
- Vulnerability scanning reports (containers, dependencies, infrastructure)

5. IDENTITY & ACCESS MANAGEMENT

- Use of managed identities across services
- RBAC model and role assignments across the platform
- Access control model for both infrastructure and application layers

6. SECRETS MANAGEMENT

- Secret inventory (mapped to usage)
- Secret rotation policies and procedures

7. MONITORING, LOGGING & ALERTING

- Monitoring dashboards (e.g., Azure Monitor, Grafana)
- Alerting rules and thresholds across key services
- Centralized logging and distributed tracing setup
- Incident response integrations (if implemented)

8. RESILIENCE & DISASTER RECOVERY

- Defined RTO (Recovery Time Objective) and RPO (Recovery Point Objective)
- End-to-end disaster recovery strategy (including regional considerations)
- Backup and restore procedures
- Evidence of DR or failover testing

10. AUDIT, COMPLIANCE & GOVERNANCE

- Centralized audit logs (access, changes, deployments)
- Governance controls (e.g., Azure Policy, policy enforcement)
- Compliance requirements (if applicable)

IMPORTANT NOTE

Where certain artifacts cannot be shared directly due to security, confidentiality, or regulatory constraints, we would appreciate the opportunity to **review them via a controlled session (screen sharing or supervised access)**. This will allow us to validate the controls without requiring sensitive data to be distributed.

Providing the above information will enable us to complete the assessment across:

- Infrastructure resilience and fault tolerance
- Security posture and risk exposure
- Scalability and performance readiness
- Operational maturity and recoverability

Please let us know if clarification is required on any of the requested items, or if alternative forms of evidence can be provided. We appreciate your cooperation and look forward to your response.