Functional Requirement Specification (FRS)
For Development of Cyber Security and Cloud Specification for the Kavach System
(Indian Railways Automatic Train Protection System)

1. Objective

The objective of this FRS is to define comprehensive policies to ensure the security, resilience, and operational integrity of the Kavach system, including all associated subsystems, by developing robust cybersecurity measures and formulating guidelines for the use of cloud services. Aligned with standards such as EN 50701, EN 50716 and IEC 62443, it will incorporate system partitioning into zones and conduits, detailed risk management processes, and threat assessment strategies to address emerging cyber threats.

The objectives include:

- Establishing a policy framework for securing the Kavach system, its processes, and interactions.
- Providing clear security guidelines for equipment development firms to ensure the secure design and development of Kavach infrastructure.
- Defining protocols for system certification and regular security audits.
- Establish a secure cyber ecosystem for Kavach.
- Ensure effective vulnerability and patch management.
- Implementing inventory and asset management mechanisms.
- Developing mechanisms for cyber incident response, audits, and crisis management.
- Mitigating supply chain risks and enhance operational security.
- Formulating guidelines for the use of cloud services.

2. Scope

The scope involves the creation of cybersecurity and cloud-based policies that:

- Apply to the entire lifecycle of the Kavach system, covering design, implementation, operations, and maintenance.
- Guide audits, inspections, and certifications conducted by empanelled firms.
- Establish mandatory practices for Kavach system integrators, equipment manufacturers, and service providers to enhance system security.

3. Prioritization

- Ensure compliance with critical standards like IEC 62443, ISO 27017, EN 50716 and EN 50701.
- Address vulnerabilities in evolving technologies, especially quantum computing and cloud storage.
- Strengthen accountability through structured documentation, testing, and monitoring practices.

4. Applicability

The selected firm shall:

- Develop detailed cybersecurity policies and guidelines for the Kavach system aligned with IT Rules 2018, IR-ICT Security Policy 2019, and sector-specific standards.
- Define security measures including firewalls, whitelisting, secure remote access, and multi-factor authentication.

- Establish specifications for secure data management, system audits, and asset management.
- Provide templates and guidelines for incident response and disaster recovery mechanisms.

5. Deliverables

The selected firm shall:

- Develop detailed cybersecurity policies and guidelines for the Kavach system aligned with IT Rules 2018, IR-ICT Security Policy 2019, and sector-specific standards.
- Define security measures including firewalls, whitelisting, secure remote access, and multi-factor authentication.
- Establish specifications for secure data management, system audits, and asset management.
- Provide templates and guidelines for incident response and disaster recovery mechanisms.

6. Functional Requirements

6.1. Cybersecurity Controls

- **Policy Formation**: Guidelines for network isolation, IP whitelisting, and trusted hardware/software sources.
- **Asset Lifecycle Management**: Detailed requirements for inventory and monitoring tools.
- **Access Control**: Role-based access mechanisms with strong authentication protocols.
- **Risk Assessment**: Conduct Detailed Risk Assessment (DRA) for zones and conduits, classify risks, and implement countermeasures to achieve acceptable residuals risks.
- **Information and Privacy Management:** Establish a comprehensive ICMS and PIMS to safeguard sensitive data and mitigate privacy threats.
- **Post Quantum Cryptography (PQC):** Implement PQC encryptors with pre-shared keys or quantum-safe certificates to secure inter-site communications.

6.2. Vulnerability and Patch Management

- Regular vulnerability assessments and third-party certifications for deployed systems.
- Risk-based remediation strategy and secure update protocols.

6.3. Backup and Disaster Recovery

- Specifications for backup mechanisms adhering to the 3-2-1 rule.
- Guidelines for disaster recovery site management and periodic validation drills.
- Use geo-redundant cloud services with strong disaster recovery mechanisms for centralized Kavach applications like FRACAS, chatbots, and version control systems.

6.4. Incident Response

- Create a cyber incident response plan, including roles, communication strategies, and reporting mechanisms.
- Maintain a Threat Log for every zone and conduit, documenting threat names, sources, potential impacts, vulnerabilities, and mitigations.

6.5. Audits and Compliance

- Define audit requirements per ISO/IEC 27001 standards.
- Procedures for penetration testing and cybersecurity audits by third-party agencies.

6.6. Cybersecurity Awareness and Training

- Specifications for comprehensive training programs tailored for all levels of employees and stakeholders.

6.7. Service Provider Management

- Include cybersecurity-related clauses in vendor/service provider contracts with penalties for non-compliance.

6.8. Secure Configuration and Change Management

- Specifications for approving and vetting configuration changes.

6.9. Cloud Services Policy

- Trusted Providers: Use certified CSPs compliant with ISO/IEC 27001 and ISO/IEC 27018.
- Data Sovereignty: Comply with national data residency laws, ensuring data storage within India where required.
- Service Continuity: Adopt automated failover and disaster recovery mechanisms with SLA-backed guarantees.

7. Annexure- R- Kavach Cloud and Cyber security requirements of Kavach Specification is enclosed. Comments on this document are to be provided.

Digitally Signed by Pavan
Kumar Gudavalleti
Date: 28-04-2025 12:34:40
Reason: Approved