Data Security Policy and Implementation Framework

Author: Rohit M / Vidya S

Date: 22-Oct-2024

Introduction

Reput is a SaaS platform that aggregates data and insights from global hybrid systems to provide sustainability-related, verified information. Certified ESG (Environmental, Social, and Governance) data flows through the platform, ensuring trust-based transparency. Reput is designed to give brands and manufacturers a One-View EPR/ESG scoring system along with drill-down data for detailed analysis.

Key features include:

- - Automated data collection and reporting for seamless insights.
- - Trust-based, self-governed data verification to validate entries from lower nodes.
- - Efficiency enhancement by integrating with existing systems to streamline operations.

Technology Framework and Principles

Self-Sovereign Identity (SSI)

SSI architecture ensures secure data exchange and verification at various levels:

- - Supplier Onboarding: Verifies ESG certificates for sustainable operations.
- - Master Data Management: Manages core data across the supply chain.
- - Supply Chain Collaboration: Facilitates shared responsibility on sustainability goals and human rights policies.

Data Protection and Best Practices

a. AWS Cloud Security

AWS is the core hosting platform, ensuring scalable, secure infrastructure:

1. 1. Information Classification: Data is categorized as confidential or classified, with access restricted to authorized personnel only.

2. 2. IAM Controls: AWS Identity and Access Management (IAM) enforces granular permissions on services like S3 and RDS.
3. 3. Encryption Standards: AES-128 or AES-256 encryption protects data at rest, applied to storage layers like Amazon Elastic Block Storage (EBS) and Amazon RDS.
4. 4. Versioning & Auditing: Services like Amazon S3 include versioning and logging to track data changes via CloudWatch.
5. 5. Backup and Disaster Recovery: Data is replicated across Availability Zones to ensure continuity.

b. Endpoint Security Policies

To secure all endpoints, strict policies are enforced on both Windows and Linux/Mac OS systems.

- Windows Systems:
    - Password policies aligned with internal security standards.
    - Audit logging enabled to track user actions.
    - Account lockout features to prevent brute-force attacks.
    - Screen lock enforced on idle timeout.
    - Auto-run disabled for external devices to block unauthorized execution.
    - Local guest users disabled, and administrative accounts renamed for security.
    - Windows Firewall enabled unless endpoint security software includes firewalling.
- Linux/Mac OS Systems:
    - Admin passwords managed by IT for all systems.
    - Regular audits to check for compliance with lockout policies and screen locks.
    - System firewalls enabled for comprehensive protection.
    - Guest accounts disabled, and admin accounts renamed for consistency.

Network DLP & HTTP Proxy Policies

Key controls include:

- Uploading to external web services (e.g., email, file-sharing) is restricted.
- Downloads of unauthorized software are blocked or logged for review.
- All data is stored in the cloud to minimize local storage risks.

Employee Training & Awareness Programs

Employees undergo regular awareness sessions to ensure familiarity with security protocols:

- Confidentiality: Protecting data from unauthorized access.
- Integrity: Ensuring data remains accurate and unmodified.

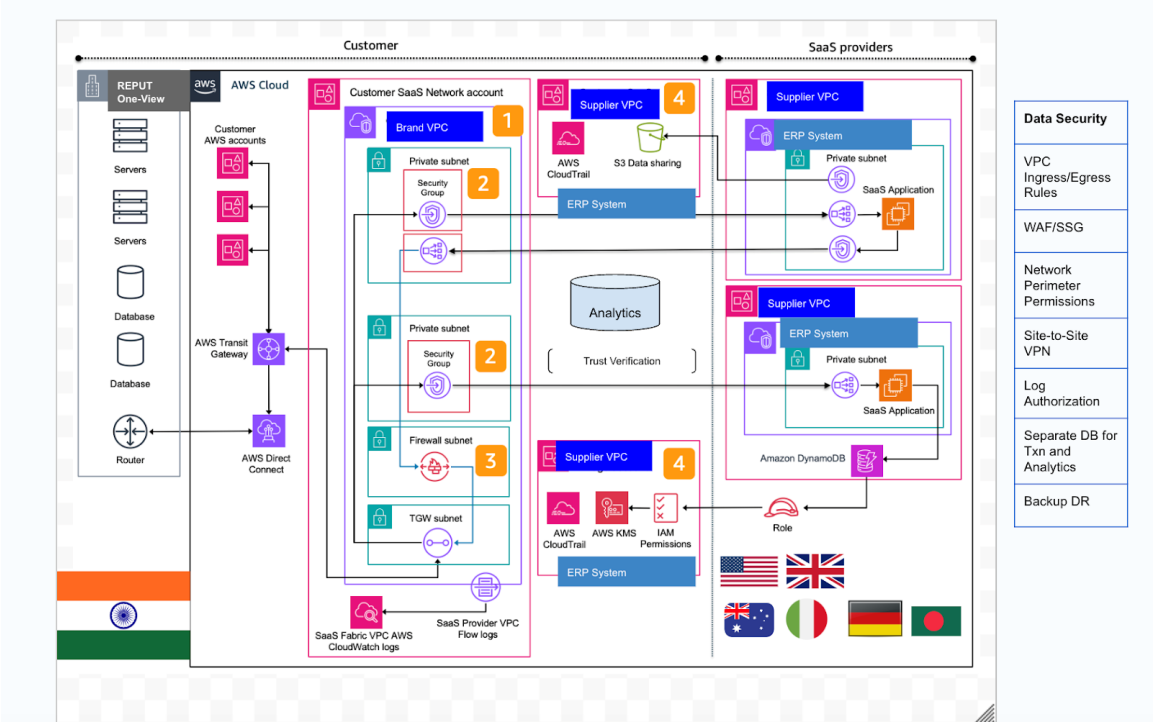
- Availability: Guaranteeing users can access information when needed.

Specific Topics in Awareness Sessions:

- Acceptable Usage Policy
- Physical Access Control
- Security Incident Management Procedures
- Clean Desk & Clear Screen Policy
- Password Management Guidelines
- Cloud Hardening Protocols
- Antimalware Policy & Controls
- Internet Usage Policy
- Document Management Procedures
- Access Control Policy

Hosting, Deployment, and Security Controls

The Reput platform follows a SaaS Hyperledger Architecture to maintain transparency, security, and scalability. Cloud deployment includes multi-zone redundancy, continuous monitoring through CloudWatch, and automated scaling.



Compliance with Data Protection Laws

Reput complies with local and international data privacy regulations:

- Information Technology Act, 2000 (India)
- Sensitive Personal Data or Information Rules, 2011

Certifications and Audits

- ISO/IEC 27001: Information Security Management
- CERT-IN Compliance: Computer Emergency Response readiness
- STPI (Software Technology Parks of India) certification for IT compliance

End User License Agreements (EULA)

- License Terms: Defines usage rights but not ownership of the software.
- Prohibited Activities: Prevents users from leasing, distributing, or modifying the software.
- Legal Consequences: Unauthorized use will result in penalties under relevant laws.
- User Acceptance: The EULA must be accepted before users can access the platform.

Website and Content Security

- Usage Rights & Restrictions: Clearly outlined in the terms of use.
- Ownership: Content and intellectual property remain with the platform.
- Fees and Payment Terms: Detailed in the service agreement.
- Data Confidentiality & Security: Assured by robust encryption and user access controls.
- Liability Limitations: Specified to manage risk and disputes.
- Governing Law: Jurisdiction-specific laws will apply to disputes.

Note : We have appointed a Data Protection Officer (DPO). Below are the details

Name: Sudalagunta Nagendra Babu
Email: nagendra@reput.co.in
Phone: 8985408020

Any other details please visit our website https://www.reput.ai