

Policy on Minimum Information Security Requirements for Vendors

AAR Insurance (K) Ltd

1. Purpose

This policy establishes the minimum information security requirements for all vendors, contractors, consultants, and third-party providers ("Vendors") who create, receive, store, process, or transmit AAR Insurance (K) Ltd.'s confidential, personal, or sensitive information.

Ensuring vendor compliance is vital to protect the security, confidentiality, and integrity of customer information and to meet regulatory obligations (including but not limited to GDPR, HIPAA, GLBA, and state insurance regulations).

2. Scope

This policy applies to:

- All Vendors engaged in services or products that involve access to AAR Insurance (K) Ltd data.
- All subcontractors used by Vendors for services involving such data.

3. Information Security Requirements

3.1 Data Governance and Classification

- Vendors must classify all AAR Insurance (K) Ltd data based on sensitivity (e.g., Public, Internal, Confidential, Highly Confidential).
- Vendors must apply controls commensurate with the data classification level.
- Sensitive data includes Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Information (PCI), financial data, and insurance policy details.

3.2 Data Protection Measures

- Data must be encrypted in transit (TLS 1.2 or higher) and encrypted at rest (AES-256 or higher).
- Portable media containing sensitive data must be encrypted.
- Data masking, anonymization, or pseudonymization techniques must be applied where feasible.

3.3 Access Management

- Access to AAR Insurance (K) Ltd data must follow the principle of least privilege and role-based access controls (RBAC).
- Multi-Factor Authentication (MFA) is mandatory for administrative access and systems processing sensitive data.
- A formal user provisioning and de-provisioning process must exist, including quarterly access reviews.

3.4 Secure Software Development (where applicable)

- Vendors must adopt secure coding practices (e.g., OWASP Top 10 compliance).

- Source code with AAR Insurance (K) Ltd integrations must be protected via version control with restricted access.
- Vulnerability scanning and code reviews must be conducted before deployment.

3.5 Network and Infrastructure Security

- Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and endpoint protection solutions must be in place.
- Systems must be regularly updated and patched (within 30 days for critical vulnerabilities).
- Administrative access must only be permitted through secure channels (e.g., VPNs, bastion hosts).

3.6 Monitoring and Logging

- Vendors must maintain centralized logging for all systems processing AAR Insurance (K) Ltd data.
- Logs must be protected from tampering and retained for a minimum of 12 months.
- Regular monitoring and anomaly detection must be performed to identify unauthorized activities.

3.7 Incident Detection and Response

- Vendors must maintain a written Incident Response Plan (IRP).
- Vendors must notify AAR Insurance (K) Ltd of any actual or suspected security breach involving its data within 24 hours.
- A formal Root Cause Analysis (RCA) must be submitted within 10 business days after an incident.

3.8 Business Continuity and Disaster Recovery

- Vendors must maintain documented Business Continuity (BC) and Disaster Recovery (DR) plans.
- BC/DR plans must be tested at least annually and results documented.
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical services must meet AAR Insurance (K) Ltd's expectations.

3.9 Physical Security

- Facilities housing AAR Insurance (K) Ltd data must have physical access controls (e.g., badging systems, visitor logs, CCTV).
- Sensitive areas must be restricted to authorized personnel only.

3.10 Personnel Security

- All Vendor personnel accessing AAR Insurance (K) Ltd data must:
 - Pass background checks appropriate to the level of access.
 - Sign confidentiality agreements before access is granted.

- Complete annual security and privacy awareness training.

3.11 Subcontractor Management

- Vendors must not engage subcontractors to handle AAR Insurance (K) Ltd data without prior written consent.
- Approved subcontractors must meet all the same information security requirements.
- Vendors remain fully liable for the acts and omissions of subcontractors.

3.12 Privacy Compliance

- Vendors must comply with all applicable data protection laws (e.g., GDPR, CCPA, HIPAA, GLBA).
- Vendors must support Data Subject Access Requests (DSARs) if applicable (e.g., data access, correction, deletion).

3.13 Data Retention and Secure Disposal

- Vendors must retain AAR Insurance (K) Ltd data only as long as necessary to meet contractual and legal requirements.
- Secure deletion methods must be used (e.g., DoD 5220.22-M standard, NIST 800-88 guidelines).
- Upon contract termination, all data must be securely deleted or returned, with certification of destruction provided.

4. Compliance, Audits, and Penalties

- Vendors must provide evidence of compliance upon request (e.g., SOC 2 Type II reports, ISO 27001 certification, external audit reports).
- AAR Insurance (K) Ltd reserves the right to audit or assess Vendors' compliance on an annual basis or as needed.
- Non-compliance may result in contract suspension, termination, financial penalties, and legal action.

5. Contacts

For questions regarding this policy or to report a security incident:

Group Head of Technology

Name: Eugene Sanya
Email: esanya@aar.co.ke;
Phone: +254 703 063 000

Acknowledgment

Vendor hereby acknowledges receipt of this policy and agrees to comply fully with the Minimum Information Security Requirements as a condition of its engagement with AAR Insurance (K) Ltd.

Vendor Name: _____

Authorized Signatory: _____

Date: _____

Vendor Information Security Self-Assessment Questionnaire (VSAQ)

Instructions:

Vendors must complete this questionnaire truthfully and completely. Supporting documentation may be requested for verification.

Section 1: General Information

Item	Response
Vendor Company Name	Strategic Business Solutions Limited
Primary Contact Name	Mauncho Felix
Title	Head Of Innovations & Technology
Email	felix.mauncho@sbsl.co.ke
Phone Number	+254722540169
Nature of Services Provided to AAR Insurance (K) Ltd	Collection, retrieval, extraction, transformation, migration, storage, validation, access control setup, and secure transfer of Personal Data between systems.

Section 2: Information Security Program

1. Do you have a formal, documented information security program?
 - Yes
 - No
 - If yes, please provide a summary.

The SBSL Information Security Program is anchored on five core objectives that are designed to provide comprehensive protection for the company's information assets. It is centered around the foundational principles of ensuring:

- data confidentiality (preventing unauthorized access)
- maintaining data integrity (ensuring accuracy and completeness),
- guaranteeing availability (making sure data is accessible to authorized users when needed).

The program commits to upholding compliance with all relevant legal and regulatory frameworks, including the Kenyan Data Protection Act, and aims to achieve operational resilience by minimizing the potential business impact of any security incidents.

2. Are you certified in any of the following? (check all that apply)
 - ISO/IEC 27001
 - SOC 2 Type II
 - PCI DSS

- HIPAA / HITECH
 - Other: _____
3. Is your organization subject to GDPR, HIPAA, GLBA, or other privacy laws?
- Yes
 - No
 - If yes, specify which.

Section 3: Data Protection

4. Is all sensitive customer data encrypted at rest?
- Yes
 - No
5. Is all sensitive customer data encrypted in transit?
- Yes
 - No
6. Do you implement data minimization and retention policies?
- Yes
 - No
7. Do you maintain documented procedures for secure data disposal?
- Yes
 - No

Section 4: Access Controls

8. Do you enforce Multi-Factor Authentication (MFA) for access to sensitive systems?
- Yes
 - No
9. Are privileged accounts managed separately from standard accounts?
- Yes
 - No
10. Do you conduct access reviews at least quarterly?
- Yes
 - No

Section 5: Risk Management and Incident Response

11. Do you conduct regular vulnerability scans on your systems?

- Yes
- No

12. Do you perform annual penetration testing?

- Yes
- No

13. Do you have an Incident Response Plan (IRP)?

- Yes
- No

14. Can you notify AAR Insurance (K) Ltd within 24 hours in case of a breach involving our data?

- Yes
- No

Section 6: Subcontractors

15. Do you use subcontractors to deliver the contracted services?

- Yes
- No

16. If yes, do subcontractors adhere to the same security standards?

- Yes
- No

Section 7: Business Continuity

17. Do you have a documented and tested Business Continuity and Disaster Recovery Plan?

- Yes
- No

Certification

I hereby certify that the information provided in this questionnaire is accurate and complete to the best of my knowledge.

Authorized Signatory Name: _Felix Mauncho

Title: Head of Technology & Innovations

Date: 11th July 2025

Signature

A handwritten signature in black ink, appearing to read "Felix Mauncho".