

## **Salaam African Bank Information Security Policy Statement**

Salaam Bank is committed to maintaining and improving information security and minimizing exposure to risk within the bank to provide secure and quality services to their customers.

Salaam Bank is committed to:

### **1. Maintaining Acceptable Risk Levels**

Information security risks will be identified and mitigated to remain within acceptable levels for Salaam.

### **2. Risk Management of Changes and Third Parties**

Risks arising from organizational, physical, environmental, technological, or third-party changes will be assessed and managed effectively.

### **3. Confidentiality and Integrity Assurance**

Corporate and customer information confidentiality will be safeguarded, unauthorized access prevented, and information integrity maintained.

### **4. Controlled Information Access**

Information will only be accessible to authorized individuals, processes, or entities as needed, ensuring compliance with legal, contractual, and regulatory requirements.

### **5. Integration with Business Continuity**

The security of information will be prioritized during the development, maintenance, testing, and invocation of business continuity plans.

### **6. Incident Management**

All information security breaches will be reported and addressed following documented incident management procedures.

### **7. Least Privilege Access**

Access to information will adhere to the principle of least privilege to minimize risk.

### **8. Compliance Commitment**

Salaam African Bank will ensure compliance with all relevant legal and contractual information security requirements.

## **Information Security Objectives**

These objectives define actionable, measurable goals to align with the policy statements and drive continuous improvement:

### **1. Risk Mitigation**

Identify, assess, and maintain risks at levels acceptable to Salaam, continuously monitoring and improving controls.

### **2. Third-Party Risk Management**

Conduct regular assessments of risks associated with third parties and ensure remediation of identified vulnerabilities.

### **3. Confidentiality Assurance**

Prevent unauthorized access and protect sensitive corporate and customer information.

### **4. Regulatory and Legal Adherence**

Meet all regulatory, legal, and contractual requirements for information security.

### **5. Continuity Planning**

Incorporate robust information protection strategies into business continuity processes for mission-critical operations.

### **6. Awareness and Training**

Deliver ongoing information security awareness and training to employees and suppliers as necessary.

### **7. Incident Response**

Reduce response time to security breaches by following structured incident management procedures.

### **8. Access Control Optimization**

Regularly review and enforce least privilege access controls for all users.

**End**