First Bank of Acmeland Security Policy

By: Andrew Waddell

19 July 2023

NTS 310 Social Engineering

# First Bank of Acmeland Information Security Policy

1. Introduction

1.1 Purpose

* The purpose of this Information Security Policy is to establish comprehensive guidelines, standards, and procedures to safeguard the information assets of First Bank of Acmeland (FBAM) and ensure the confidentiality, integrity, and availability of data.

1.2 Policy Scope

* This policy applies to all employees, contractors, vendors, and third parties who have access to FBAM's information systems and data.

1.3 Policy Framework

* This policy is designed to align with the principles and practices of the Department of Defense's (DoD) information security policies to ensure the highest level of security for FBAM's operations.

2. Information Security Governance

2.1 Information Security Management

2.1.1 Chief Information Security Officer (CISO)

* FBAM will designate a Chief Information Security Officer responsible for overseeing the bank's information security program.

2.1.2 Information Security Committee

* An Information Security Committee will be established to provide oversight, guidance, and support for information security initiatives.

2.2 Risk Management

2.2.1 Risk Assessment

* FBAM will conduct regular risk assessments to identify, evaluate, and mitigate information security risks.

2.3 Compliance

* FBAM will comply with all applicable laws, regulations, and industry standards related to information security, including financial regulations.

3. Information Security Controls

3.1 Access Control

3.1.1 User Access

* User access to information systems will be granted based on the principle of least privilege.
* Access rights will be reviewed and updated regularly.

3.1.2 Authentication and Authorization

* Strong authentication mechanisms will be used for user authentication.
* Authorization rules will be enforced to control user access.

3.2 Data Protection

3.2.1 Data Classification

* Data will be classified based on its sensitivity and importance.
* Access controls and encryption will be applied accordingly.

3.2.2 Encryption

* Sensitive data in transit and at rest will be encrypted using industry-standard encryption algorithms.

3.3 Incident Response

* FBAM will establish an incident response plan to detect, respond to, and recover from security incidents.
* Incidents will be reported promptly to the CISO and documented.

3.4 Security Awareness and Training

* All employees, contractors, and third parties will receive information security awareness and training to ensure they are aware of their responsibilities and best practices.

4. Information Security Monitoring

4.1 Continuous Monitoring

* FBAM will implement continuous monitoring processes to detect and respond to security threats in real-time.

4.2 Logging and Auditing

* All information systems will generate and retain logs for auditing and monitoring purposes.
* Logs will be regularly reviewed for security events.

5. Security Review and Assessment

5.1 Security Audits

* Periodic security audits and assessments will be conducted to evaluate the effectiveness of security controls.

5.2 Vulnerability Management

* Vulnerability assessments and patch management processes will be in place to address security vulnerabilities.

6. Security Threats and Controls

6.1 Physical Security

6.1.1 Physical Theft

* Access to sensitive areas and equipment must be controlled and monitored.
* Sensitive physical assets (e.g., servers, data centers) must be secured when not in use.

6.2 Cybersecurity

6.2.1 Hacking

* FBAM will implement robust cybersecurity measures to protect against hacking attempts.
* Regular vulnerability assessments and penetration testing will be conducted.

6.2.2 Social Engineering

* Employees must be trained to recognize and report social engineering attempts.
* Verification procedures will be in place for requests involving sensitive information.

6.3 Email Security

* All email communications must adhere to secure practices.
* Email attachments and links will be scanned for malware and phishing attempts.

6.4 Phone Security

* Employees must exercise caution when discussing sensitive information over the phone.
* Secure communication channels will be used for sensitive discussions.

6.5 In-Person Security

* Visitors to FBAM premises must be logged and escorted.
* Employees should challenge unfamiliar individuals in restricted areas.

6.6 Misuse of Company Resources

* The use of FBAM resources for personal purposes will be monitored.
* Employees are expected to report any suspected misuse of resources.

7. Penalties

* Violations of this Information Security Policy may result in disciplinary actions, including but not limited to warnings, suspension, or termination.
* Serious violations or breaches may lead to legal action.

8. Compliance

* FBAM is committed to full compliance with all applicable laws, regulations, and industry standards related to information security, including financial regulations.

9. Conclusion

* This Information Security Policy reflects FBAM's unwavering commitment to preserving the security and confidentiality of its information assets. It will be reviewed annually and updated as needed to adapt to evolving threats and technologies.