**Information Security Policy**

**Introduction:**

X Bank's information security policy defines a number of measures that must be implemented throughout the bank to protect the bank’s information assets and information systems.

The availability, integrity and confidentiality are main principals to enhance the security posture, ensure the business continuity and to maintain the legal compliance with the regulations. Other requirements are outlined in the policy such as authentication, identification, authorisation, accountability, and accounting to support the main principals.

**Scope:**

Scope of this information security policy applies to all areas of the bank’s operations where the data is used, processed, stored, and transmitted in any format (electronic or paper … etc). This must include all X bank’s employees (including interns), third-party, partners and any entity that is dealing, generating, storing, or retrieving data.

**Objectives:**

This policy's goal is to provide all entities (all X bank’s employees, third-party and contractors) with plans to manage the risks related to the information assets and systems. The policy goal can be achieved by implementing steps such as:

1. Ensure the integrity, availability, and confidentiality of customers’ data that the bank receives, processes, stores, and transmits all time.
2. Assure adequate protection of Bank information assets, customer data and information systems against potential threats or risks to their security or integrity.
3. Secure customer and bank information assets and systems against unauthorised access or use that could cause serious harm or annoyance to any customers or put the bank's safety at risk.
4. Provide an immediate detection and evaluation of any vulnerabilities or threats that could impact the security or integrity of client and bank information assets and systems.
5. Establish criteria for testing the Policy, and modify it to meet the technological advancements, the sensitivity of consumer data, and internal or external risks to information assets and systems.
6. Validate that the Bank abides by all applicable laws, rules, agreements, and conventions in Canada, the U.S, Europe, and Asia pacific that govern the security and confidentiality of customer information.
7. X Bank along with all relevant entities must comply with the adopted policies underneath this one, such as:
8. Business continuity plan.
9. Information assets acquisition and disposal.
10. Access control policy.
11. Incident response and recovery.

**A list of roles and corresponding responsibilities:**

1. **The Board of directors of the organization:**

The board of directors are responsible for:

* Ensuring the security policy, program and strategy are effective, efficient, and aligned with the bank’s principals.
* The board must review, approve the policy, and oversee the implementation.
* Verifying an annual evaluation of risks and threats are in place.
* Carefully considering regulatory reviews of information security and make sure the right steps are done to address applicable laws and regulations related to information security in Canada, the U.S, Europe, and Asia pacific.
* Making sure the bank has incident response plan to detect, respond and recover in case of security incident. Along with allocating adequate resources in case of incident.

1. **The president/CEO:**

The president/CEO is accountable for:

* Overall leadership to ensure that the bank's information security policy and program are effective and implemented correctly.
* Establish a framework with the employees, third parties and customers and provide them with unique experience on how to keep their data private and confidential.
* Verify the risk management program and the mitigation strategies in case of incident.
* The CEO must lead the organization's culture of information security awareness and compliance and get updates on the information security program.
* Ensuring the bank is compile with all regulation laws and standards.

1. **The CISO:**

The chief information security officer is responsible for:

* Protecting and ensuring the Confidentiality, Integrity, and availability of the bank’s information assets and systems.
* The CISO must work closely with the other departments such as HR, compliance, risk management, asset management, communication, and other teams to ensure the security program is aligned with the bank principals and strategies.
* The CISO must develop information security plans, standards, procedures, and guidelines that allow the bank to adjust with the risks and the ever-changing regulatory compliance such as PCI DSS, PIPEDA, GDPR .. etc.
* Manage the daily security operations of the bank.
* CISO must develop, participate in creating inclusive information security strategy, this strategy must adhere with the lifecycle of information security operations. For instance:
* Threat intelligence.
* Following and monitoring reports from auditors and cybersecurity reporters.
* Managing the risks how to mitigate it.
* Develop, publish, adopt, and review policies such as business continuity plan and incident response plan.
* Ensure that company employees understand security measures and include them in some sort of coaching and awareness.
* Managing third-party communication and the risks associated with accessing the bank's information assets and systems to ensure they comply with the bank policies.
* Make sure the information security program is aligned with the guiding principles of the bank.

1. **Audit committee:**

The audit committee is responsible for:

* Review and approve the security policies, standards, and guidelines.
* Conduct proper tests and audits of the information security systems, programs and controls to ensure they are efficient and effective.
* Review the reports to ensure the right action is taken in case of weaknesses in the system.
* Analyze and examine the third-party communication and looking for any control weaknesses.

1. **Information security officer:**

He is responsible for:

* Performing risk assessments to identify potential information and information system threats and weaknesses and creating and putting in place suitable controls to reduce such risks.
* Detect and address security issues by monitoring and analysing logs and perform alerts.
* Ensuring the overall compliance with the Bank's information security procedures and policies are effective, and the risks are assessed.
* Participating in incident response planning and carrying out incident response procedure.
* Assure the policies and procedures in place to protect against such risks are adequate.
* The ISO is responsible to report in case of breach to the board and any regulatory and law enforcement agencies.

1. **Information security administrator:**

He is responsible for:

* Approving and implementing information system user access permissions.
* He is also in charge of maintaining and reviewing information security systems and associated reports.
* Notifying the Security Officer and ISO of any attempted or successful security system breaches.
* Protect the bank’s information assets and system by deploying security tools such as anti-malware, anti-virus firewall and IDS.
* Monitor and analyse system logs and detect any suspicious event.

1. **HR:**

HR department is accountable for:

* Guaranteeing new hires receive the proper information security orientation.
* Verify that all new hires and contract employees have undergone a thorough background check.
* New employees have agreed and signed the acceptable usage policy and abide by Bank information security rules.
* Verify that employees adhere to bank policies and that the bank's data is kept secure following termination or retirement.

1. **Branch managers:**

Branch managers are responsible for:

* Make sure staff members are securing client information with proper protection.
* Report any data breach to the Information security administrator and the Information security officer.

1. **X bank employees:**

All X bank employees are responsible for:

* Protecting customers’ data on daily basis.
* Report any data breach to their respective managers.

**Policy statement:**

In order to protect its information assets and systems, the bank's information security policy defines the rules and regulations it must comply with. The main domains of the ISO 27001 must be implemented. (The new version of ISO 270001 has four category and 98 domains, but we still go with the 2013 version that have 14 domains).

1. **Information security policies:** develop, implement, maintain, and improve the information security policies to protect the confidentiality, integrity, and availability of the information assets and systems and modify it at least once a year or as needed.
2. **Human resources security:** ensure that all its employees and third-party are trained and qualified for their roles in relation to the bank’s information security policies.
3. **Access control:** implementing access control to prevent unauthorised access to the bank’s information systems and critical sites.
4. **Physical and environmental security:** preventing unauthorised access to the critical sites.
5. **Operations security:** maintain secure operations to the bank processes.
6. **Supplier relationships:** third parties security maturity must meet or exceed the bank’s security posture.
7. **Information security aspects of business continuity management:** a documented business continuity plan must be in place to maintain the availability during and after disruption.
8. **Organisation of information security:** develop a management framework to initiate and manage the implementation of the information security within the bank.
9. **Asset management:** The goal is to identify the information assets that fall under the management system's scope and to specify the proper levels of security.
10. **Cryptography:** ensure the utilisation of cryptography properly and effectively to secure the data while its stored or transmitted in a physical server or on a cloud.
11. **Operations security:** maintaining the secure and appropriate operation of data processing infrastructure.
12. **System acquisition, development and maintenance:** ensure the security is core component of the information system throughout its lifespan.
13. **Information security incident management:** a clear and efficient approach to the lifecycle of incidents, events, and weaknesses is in place. A policy must be clear on how to respond to any incident and recover and back to normal operation as soon as possible.
14. **Compliance:** legal and legitimate criteria must meet. The goal is to prevent violations of any information security-related legal, statutory, regulatory, or contractual demands.

**Applicable laws and regulations:**

X Bank is governed by a number of information security-related rules and regulations in Canada, the U.S, Europe and Asia pacific. Some of the laws and rules that X Bank must abide by in Canada and Europe are as follows:

1. Bank act (Canada): The Bank Act is a federal law that controls how banks and other financial institutions that operate in Canada. The Bank Act contains laws relating to the security of electronic banking services, the confidentiality of banking information, and the protection of costumers’ information.
2. Office of the Superintendent of Financial Institutions (OSFI) (Canada):

Recommendations and guidelines for managing cyber risk and information security for banks.

1. Personal Information Protection and Electronic Documents Act (PIPEDA)(Canada):

Federal law defines rules for use, collect and disclose any personal data by any organisation in Canada. It also requires implementing secure procedures to protect the personal data.

1. Canadian Anti-Spam Legislation (CASL):

The bank must abide by this federal law when sending marketing messages or email to its customers.

1. Payment Card Industry Data Security Standard (PCI DSS):

To protect its customers from fraudulent use of credit and debit cards, X Bank must adhere to the PCI DSS security standards.

1. Global Data Protection Regulation (GDPR) (Europe):

Since X bank operates in Europe, the bank must adhere with GDPR law. The use, collection, and disclosure of personal data in Europe are all regulated by this law.

1. In the U.S. the bank must adhere with the following laws:
2. Gramm-Leach-Bliley Act
3. Sarbanes-Oxley Act
4. Fair Credit Reporting Act
5. Electronic Funds Transfer Act
6. Computer Fraud and Abuse Act
7. The bank must adhere with other laws in provincial and state jurisdictions.

**Compliance to the policy (verification requirements:**

To ensure adherence to this Policy, X Bank has created an extensive information security program that is suitable and relevant to the threats and vulnerabilities the bank faces as well as the nature and scale of its processes. The information processing facilities use must adhere to the authorized use and information security policies. Although X Bank respects the privacy of its staff members, an acceptable usage policy outlines the right to audit and keep an eye on their actions and any information that is stored, processed, communicated, or handled on any assets, devices, or services that they use.

Information security officer has been hired to ensure compliance to this policy. The ISO will work closely with information security administrator and other teams to execute the information security program. They all will also be responsible for detection of attempted or successful security breaches, reporting of such incidents, other information security program components, applicable Bank policies, and legal and regulatory obligations. The information security program also outlines the violation of its policies and its consequences.

Practices must be carried out to verify that the information security policies, processes, and standards are being followed.

**Exceptions:**

The exception management process must be handled by the information security department and used to authorise any exceptions to security policy and procedure. Policy exceptions must be evaluated and reviewed based on developing threats, security risks, and other factors.

**Requirements regarding the update, revision, and the approval of the policy:**

The policy must be reviewed and updated at least once a year or as necessary to comply with regulatory or bank environment changes and to ensure its efficiency and effectiveness. Before updating the policy, questions must be in place on why we need to update the policy, who asked for the update, and how it will change. It's crucial to inform all relevant parties, including employees, contractors, and third-party service providers, of any changes to the policy after it has been updated or altered. It should be outlined in the policy how updates will be made and how awareness of the policy will be kept up to date.Eventually, the policy must be approved by the CEO and the Board of Directors.

**Glossary:**

1. information assets: according to NIST the information assets mean, “A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems”.
2. information systems: combination of hardware and software to process, store and transmit data.
3. Threat: weakness in the system has been exploited. Potential even could cause hard to the system or the organisation.
4. Vulnerability: weakness in the system might be exploited to damage the system.
5. Threat intelligence: it’s the gathering, analysing, and sharing information on present and potential cyberattacks that could threaten the assets of an organisation.
6. Access control: is the process of identifying user with given credential and authenticate him to get authorised access to a system.

**Version control:**

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Samer Mahmoud | | |
| Document Name | Information security policy | | |
| Version | 1.0 | | |
| Source | X bank information security | | |
| Policy owner(s) | Information security department at X bank | | |
| Date | Version | Author | Changes/comments |
| 23/3/2023 | 1.0 | S.M | Final version approved by CEO and the board of directors. |