Burgan Bank

Information and Cybersecurity Management Policy

بنک برقان
BURGAN BANK

Introduction

This booklet has been developed by and is the exclusive property of Burgan Bank. Any attempt to copy, duplicate or modify this booklet may be considered an act of forgery and may be the subject of criminal proceedings. This booklet is given to every director, executive and employee of Burgan Bank, and the guidelines mentioned herein are considered by Burgan Bank as a necessary code of ethical behavior and good conduct to be strictly adhered to and followed by all such directors, executives, and employees of Burgan Bank; each of whom has a duty to conduct him/herself based on the principles of good faith and integrity.

Policy Statement

Information and data are considered to be one of the crucial assets of any banking and financial services organization. Data breaches occur regularly which involves unauthorized access, modification or disclosure of confidential information relating to customers, stakeholders and employees. These data breaches, depending on the severity and its impact, can lead to loss of confidential information, financial losses operation disruptions and regulatory non-compliance.

Protecting and securing such information and data is becoming one of the key activities of any bank. It is imperative for banks to protect and ensure 'Confidentiality', 'Integrity', and 'Availability' of its information assets and technologies that process them. This requires an effective and efficient 'Cyber Security' program to identify protect defend and monitor cyber security activities in a structured method. One of the important enablers of the Cyber Security program is this policy.

Burgan Bank ("the Bank") has developed this information and Cyber Security Policy as this policy to convey the intention of Board of Directors ("BOD") and Senior Management in directing, governing, managing controlling the information and data assets of the Bank, all in line with the regulations and the applicable best practices.

PURPOSE

The purpose of this policy is to provide cyber security strategy and governing principles for the Bank's Information and Cybersecurity (ICSD) to develop adequate programs and manage its activities. The main purpose of the Policy is to:

- Establish an effective Information and Cyber Security program for the Bank;
- Establish a governing structure defining roles, responsibilities and accountabilities for action and/ or inaction of various stakeholders, and the consequences of non-adherence to the Policy;
- Align security practices with business objectives;
- Ensure compliance with regulatory, legal, and industry standards; Foster continuous improvement in security policies and controls;
- Institute and implement various appropriative Information and Cybersecurity control measures to ensure confidentiality, integrity and availability of information and data assets;
- Ensure that the Bank's security control requirements are defined by carrying out Risk Assessments at periodical intervals and by selecting and implementing appropriate Risk Treatment Plans;
- Set minimum security baseline standards that need to be configured while

implementing Banking Application systems and infrastructure components;

- Develop and sustain methodologies and frameworks to integrate and coordinate governance, Risk, and Compliance initiatives within business processes;
- Provide a holistic view of the current Governance Risk Compliance ("GRC") posture with respect to Information and Cyber Security to make informed decisions to manage cyber risks effectively;
- Ensure continued availability of Banking Application Systems and infrastructure to support uninterrupted banking services to the Bank's customers; and
- Establish process for cyber security incident detection, response, and recovery

This Policy shall be read in conjunction with all applicable regulation, legal and compliance mandate, including but not limited to internal policies, industry standards, CBK's 'Cyber Security Framework ("CSF") and Cyber Security Baselines ("CSB") and Standards such as International Organization for Standardization ("ISO") 27001:2022 and 27701:2019 and Payment Card Industry Data Security Standard ("PCI-DSS").

The Policy is applicable to all of the Bank's employees, as well as outsourced employee. Each relevant department will ensure that engagement letters with third-party services providers (including third party information processors) include provisions that pertain to the obligations of the service providers and their staff and employees to abide by terms and conditions substantially similar to those set out in this Policy and the Rules.

The Policy requirements are not only extended to electronically stored and processed information and data, but also equally applicable to hardcopy information, video and pictures, and messages that are orally communicated.

This Policy including any information and data contained herein (the "Content") may be shared with the Bank's subsidiaries for reference and guidance only and for the purpose of the development of the respective Subsidiary's own policies and procedures in connection with Cyber Security (the "Permitted Purpose"). Each Subsidiary, by receipt hereof and access hereto, agrees to solely use the Policy and content for the Permitted Purpose and treat them in strict confidence. Each Subsidiary may only share the Policy and the content with its respective staff and employees who need to know the same for the permitted purpose.

RESPONSIBILITIES

The bank has adopted a three-tiered risk management structure to ensure effective governance and oversight of information security risks. The first line of defense consists of business and operational units responsible for implementing security controls, ensuring compliance with policies, and managing operational security risks within their functions. The second line of defense, led by the ICSD-Risk Management department, provides independent oversight and advisory, conducts risk assessments, and ensures security policies align with regulatory and industry standards. The third line of defense, the Internal Audit function, conducts independent assurance reviews to assess the effectiveness of security controls and governance. This structured approach ensures clear accountability, continuous risk monitoring, and alignment of security risk management with business objectives.

BOARD OF DIRECTORS

- The BOD will direct the Senior Management of the Bank to develop a governance structure that is suitable to provide the required direction;
- Monitor the effective functioning of the Information and Cyber Security Program and the implementation of the Policy; and control the overall performance of the ICSD.
- The ICSD, and Board Risk Committee ("BRC") of the Bank will be actively engaged in understanding and managing the Bank's cyber risk.
- The BOD / BRC will be the approving authority for the strategy, policy and other Cyber Security initiatives.
- The BOD or delegated Senior Management will approve risk tolerance levels based on the continuously evolving Cyber Security trends and threats to the information and data assets.
- They will promote continual improvement to the Bank's Cyber Security posture.
- The BOD or Senior Management shall allocate adequate Cyber Security budget; assign roles and responsibilities; and will promote Cyber Security culture at all levels within the Bank.

INFORMATION AND CYBER SECURITY DEPARTMENT (ICSD)

The ICSD will be an independent function and will report to the Chief Risk Officer ("CRO") of the Bank. It will not perform any IT operational activities and thereby shall not introduce any conflict of interest.

DATA PRIVACY, PROTECTION AND SECURITY

To ensure protection from information breaches and to create trust by responsible use of privacy data, the Bank shall establish appropriate data protection, security and privacy measures.

DATA PROTECTION AND SECURITY MEASURES

- ICSD shall define Data Protection Security controls for identification and protection of important records and these controls shall be enforced by relevant stakeholders. The policy and controls will include specifications for processing, storage, retention and disposal of important records in accordance with:
    - Regulatory and legal requirements; and
    - Local and cross-border business requirements.
- Adequate Security controls shall be implemented to protect confidentiality, integrity and availability of sensitive data and important records while at rest and in transit.
- Encryption techniques used to protect important records shall be in accordance with the cryptography controls of the Bank.
- Data security and privacy considerations / measures shall be considered and implemented for protecting data shared with supply-chain vendors.
- Data protection and privacy requirements shall be communicated to and adhered by third-party vendors, and specified in the outsourcing agreements.

DATA PRIVACY REQUIREMENTS

- Access to non-public personal information shall be limited to authorized users who need to have access to carry out the Bank's responsibilities as it relates to that information.
- Each employee and authorized user with access to confidential information shall sign a copy of the Bank's Data Privacy and Security Policy and will agree to abide by its terms.
- Processing activities shall be clearly defined in customer agreement and consent shall be obtained where applicable.

- The Bank shall not retain or process personal data beyond the original purpose unless legally required.
- Except as required by regulations / law, when the Bank provides confidential information to third-parties, it shall ensure that the necessary legal clause has been incorporated in agreement which shall mandate the third-parties to comply with the applicable provisions of its policy with respect to the non-public personal information provided.
- The bank shall enforce Data Loss Prevention (DLP) control to prevent unauthorized transmission of sensitive information.
- Personal data shared with third party shall comply with contractual, legal and regulatory requirements.
- Bank shall establish the data retention requirement based on legal, regulatory and business requirements. Personal data shall be securely disposed when no longer required.
- Audit logging and monitoring shall implement to track all the access and modification to personal data.
- Data privacy controls shall be documented, approved, implemented and reviewed periodically as per compliance requirements. International standards such as ISO 27701 should be taken into consideration while dealing with personal data and relevant control implementation.

PORTABLE DEVICE SECURITY

The Bank shall implement appropriate security measures for the portable devices to ensure that risks arising from usage of unauthorized or unprotected portable computing devices are identified, managed and mitigated.

- No portable devices shall be permitted to connect to the enterprise network unless necessary authorization is obtained from relevant authorized personal as per establish process.
- The control measures relating to portable devices defined in Bank's Acceptable Usage procedure shall be followed.
- For secured usage, the portable device should be mapped to a unique employee or third-party vendor staff.
- Prior to initial use on enterprise network or related infrastructure, all mobile devices shall be registered with IT.
- End-point encryption or containerization shall be enabled on the devices.
- Monitoring shall be enabled for all portable devices that are connected to the enterprise network.

- Installed applications on the Bank’s owned portable device shall be pre-approved by the Bank.
- All portable devices used by the bank to store confidential data shall be encrypted and monitored for compliance with security policy.

TRAINING AND AWARENESS

- ICSD along with Learning and Talent Development Department will establish a security awareness and training program for all employees and relevant third-party vendor staff (as relevant).
- ICSD shall conduct the Cyber Security awareness and simulations program on a regular basis and will ensure role-based dissemination of awareness and training.
- The curriculum for information security training shall be based on the required learning goals and objectives applicable to the various stakeholder roles and categories.
- Customers will be encouraged to report phishing mails or phishing sites or unusual behavior observed through appropriate channels identified by the Bank.
- ICSD shall monitor the effectiveness of the security awareness and training program.
- Specialized information security training sessions shall be scheduled and conducted to enable the employees, end users, and onsite consultants to effectively contribute to the implementation and improvement of the Bank's information security management system, as well as to recognize the ramifications of failing to comply with the Information security Policy requirements.
- The ICSD/LTD shall retain relevant documents as evidence of conducting security awareness and training programs.

SECURITY INCIDENT MANAGEMENT

To ensure that events generated from various technology assets are continuously collected, monitored, analyzed, and tracked for early detection, and remediation, the Bank is committed to implement appropriate security information and incident management program. This Policy sets out a program to manage security events from logging to monitoring, implementing controls to containing incidents and constantly improving upon the processes and practices.

LOGGING AND MONITORING INCIDENTS

- Logging shall be enabled on all critical technology assets on the Bank's premises and / or in cloud.
- The level of and to the extent of logging will be based on the classification of the information and risk assessment.
- Relevant log sources and logs received shall be monitored.
- The completeness and accuracy of logs shall be reviewed by IT by considering the type of incidents reported, whether sufficient information logged or not, and other similar parameters.
- Bank shall define requirements for retention of logged events, incidents that are reported, and where to be retained - on-site or off-site locations.
- All logs used for monitoring and review purposes shall be adequately protected against any tampering or unauthorized access.
- All employees, contractors and third-party users shall be made aware of their responsibility to report any information security events as quickly as possible.
- The Bank's Incident Response Team shall immediately inform the respective team to investigate the incident and take further actions as necessary.

INCIDENT DETECTION AND ANALYSIS

- IT shall develop, document, approve, implement, and constantly improve the security information and event management process to identify, track, and monitor events, issues, and incidents. The process will include criteria for:
    - Classification of an event or series of events as incident;
    - Assigning ownership;

  - Assessing whether they constitute security breach;
  - Assessing the criticality of the incident; and
  - Sharing of incident information and associated threat intelligence.
- Responses to Information Security incidents will be carried out in accordance with a predefined process and procedure to ensure that the response will not be haphazard and uncoordinated;
- Relevant message types shall be transferred automatically to a centralized security information and event management system (SIEM) where information from multiple sources may be correlated and analyzed by Security operation Center team in order to help identify significant events for security monitoring purposes.
- Security Operation Center (SOC) team shall established the necessary process and procedure to timely identify and address security anomaly related incidents. These shall incorporate the industry best practices on security incident detection, containment and response domains.
- Security logs must be reviewed regularly by the SOC team and as necessary by other interested parties specifically authorized by senior management. Any major findings identified as a result of the review shall be reported to Executive Management.
- Employees and contractors using the Bank's systems will be aware of the fact that when discovering a suspected security weakness, they shall report it immediately to IT.

INCIDENT RESPONSE

- A Cyber Security Incident Response Team ("CSIRT") or equivalent group shall be formed by the Bank to respond to security incidents. The CSIRT shall be available to respond to information security incidents or events.
- ICSD shall assist to develop a security incident containment method or processes, and make them readily accessible to CSIRT to limit / mitigate security risks.
- CSIRT shall record, track, and remediate the reported Cyber Security incidents. Remediation action will commensurate to the nature and character of the incident reported.
- Management shall give prior approval to the cyber security incident response team (CSIRT) for certain technical authority/action and agreed by the key stakeholders for taking these required actions in case of major security incident.
- Bank shall formulate the necessary for OnDemand digital forensic service to

assist during the cyber incident.

- The Bank shall report issues to appropriate internal and external authorities, including the CBK, in line with the severity of occurrences and compliance requirements.
- The Bank shall implement a process to effectively demonstrate that lessons learned from past Information Security incidents are used to reduce the likelihood or severity of future incidents.
- The Bank shall implement a continuous learning framework for minimizing the incidents and effects of the incidents.

BUSINESS CONTINUITY AND DISASTER RECOVERY

The Bank will develop an effective BCP ("Business Continuity Plan") and ("Disaster Recovery") DR program to ensure continued availability of critical IT systems and data during disaster scenarios. The plan will also embed the information security continuity requirements during such a disaster. The Bank will have a comprehensive and cost-effective IT disaster recovery plan and necessary DR infrastructure that will provide for the prompt and effective continuation of critical Banking operations and information security.

ABBREVIATIONS

Abbreviation	Description
UN	United Nations
HR	Human Rights
CRO	Chief Risk Officer
CSIRT	Cyber Security Incident Response Team
ISMS	Information Security Management System
BCP	Business Continuity Planning
DR	Disaster Recovery
PCI-DSS	Payment Card Industry Data Security Standard
CSB	Cyber Security Baseline
CSF	Cyber Security Framework
GRC	Governance Risk Compliance
BRC	Board Risk Committee
PII	Personal Identifiable Information
CBK	Central Bank of Kuwait
BOD	Board of Directors
NFC	Near Field Communication
QR	Quick Response
ICSD	Information and Cyber Security Department
LAN	Local Area Network
UPS	Uninterrupted Power Supply
ITIL	Information Technology and Infrastructure Library
Term	**Description**
“the Bank”	Burgan Bank
Sensitive data	Any data that is mandated by internal and external compliance, the legal, or the government to have additional enhanced security and privacy controls. For BBK, the sensitive data are CCD, Customer Data, Financial Transaction data, PII data & other data as identified according to Bank’s data classification process.
Portable devices	Portable devices are electronic devices that can connect to a network. These devices include smartphones, desktops, laptops, mobiles, tablets and any other network-capable devices that can transmit/receive the data.