New Development Bank

New Development Bank
Information Technology Policy

Owner:	**Information Technology Division**
Version:	2020 V1
Date:	28 March 2016

Change Log

Revision Date	Chapter	Revision Details
28 March 2016	2016 v.1.0	Change log as presented at the Board meeting held on March 28, 2016
March 2020	2020 v.1.0	Change log as presented at the 24th Board meeting held on March 24, 2020

Table of Content

Abbreviations

NDB or the Bank	New Development Bank
BOD or Board	Board of Directors
IT	Information Technology
Policy	The Information Technology Policy
ITSM	IT Service Management
ITCM	IT Continuity Management
ITSD	IT Supply and Demand

1 Introduction

1.1 Objective and Overview

The objective of Information Technology Policy (or "IT Policy", "the Policy") is to set out the framework of the IT Management of New Development Bank ("Bank" or "NDB").

1.2 Scope

The policy document and associated supplementary documents apply to all NDB locations, business divisions, business areas and roles.

The Policy has been developed to establish a framework for the Information Technology Function ("IT"), in order to create robust and systematic decision-making processes and to implement efficient internal controls to prevent and mitigate risk.

1.3 Approval of Policy and Standards

The Board of Directors ("BoD") approves the Policy, and makes amendments to it.

Vice President and Chief Administrative Officer (CAO) approves the supplementary IT Policy Standards (the Standards) to implement the Policy.

1.4 Release and Control

1.4.1 Authority

The Information Technology Department is responsible for drafting and proposing amendments to the Policy and supplementary Standards.

1.4.2 Version control and revision

In order to ensure the validity and application of the Policy, review is conducted as necessary to reflect business environment changes and/or operational updates.

1.4.3 Disclosure

The Policy is for internal use only and contains proprietary information of the bank.

2   Roles & Responsibilities

2.1   All

The Policy requires NDB staff members to:

- Understand and follow NDB IT Policy, IT Policy Standards requirements and methodology.

2.2   Information Technology Department

The Information Technology Department is responsible for:

- Release and maintenance of the IT Policy, IT Policy Standards and supplementary documents.

2.3   The BoD

The BoD oversees the IT Policy of the Bank and performs the following duties:

- Approve the IT Policy and amendments to the Policy

2.4   Vice President and Chief Administration Officer (CAO)

The VP and CAO is responsible for:

- IT Policy Standards and supplementary documents review and approval.

3 IT Strategy

3.1 Objective and Overview

IT Division develops IT strategy according to the Bank's needs. The IT strategy should be consistent with the Bank's business strategy and be compliant with the IT requirements for business operations. The IT strategy should be forward-looking and should avoid over-investment due to over-scoping.

NDB's IT strategy should reflect a centralized model for IT to ensure consistent, standardized systems and processes are followed across its various locations. The Bank should follow a cloud-first strategy, where it is applicable, to maximize the value of IT across the business and take advantage of the inherent performance, cost and scalability benefits of using such as model.

The Bank should provide sufficient financial budget and resources to support the IT strategy.

The Bank's IT strategy details are documented in the NDB IT Strategy, to be reviewed by the Chief of IT on a periodic basis to ensure it continues to be relevant and achieves its objective or servicing the wider organization.

3.2 IT Planning and Budgeting

The Bank should maintain the IT investment, required by its normal business operation, and determine the priorities and the related IT project investment, when developing the NDB annual budget.

IT investment should prioritize spending to enhance the reliability and security of IT services in the Bank and should be aligned with the overall IT strategy.

IT is responsible for preparing the annual IT plan and the IT budget based on the IT strategy and following the Bank's budget planning methodology and guidelines.

Business(es) / Function(s) are responsible for timely developing the annual IT application requirements according to the business strategy and the Bank's budget planning guidelines, to provide sufficient details to IT to ensure that the annual IT plan and IT budget are robust and accurate.

Once the annual IT plan and IT budget have been approved by NDB BoD, IT and Business(es) / Function(s) should execute the IT plan as scheduled. The Business(es) / Function(s) should refine the business requirements on a timely basis, and submit the business requirements.

4   IT Service Management

4.1   Objective and Overview

The Bank should acquire a set of specialized organizational capabilities for providing value to the business in the form of IT services. The capabilities take the form of functions and processes for managing IT services over a lifecycle, with specializations in strategy, design, transition, operation and continual improvement.

IT Service Management requirements are defined in the NDB IT Service Management (ITSM) Policy, to be approved by the NDB BoD, and the supplementary ITSM Standards.

4.2   IT Change Management

IT Change Management is determined as the addition, modification or removal of authorized, planned or supported IT services or IT service component and its associated documentation.

The goals of IT Change Management are to:

- respond to the business's changing business requirements while maximizing value and reducing incidents, disruptions and re-work; and
- respond to the business and IT requests for change that will align the IT services with the business needs.

4.3   IT Project Management

IT division develops and maintains NDB IT Project Management framework, based on the best practices and following the risk-based approach.

IT Project Management Standard provides instructions and guidance to IT Project Managers and other project stakeholders throughout the life cycle of an IT project.

4.4   IT Supply and Demand Management

IT Supply and Demand Management is a critical aspect of IT service management.

Poorly managed demand is a source of risk for the IT department because of uncertainty in demand. Excess capacity generates cost without creating value that provides a basis for cost recovery. The purpose of demand management is to detect and influence the demand that the business has on IT services.

IT division develops and maintains IT Supply & Demand Standard, as part of IT service management framework.

4.5   IT Operations

IT Operations includes the execution of all ongoing activities required to deliver and support IT services.

The scope of the IT Operations includes the services themselves, Service Management processes, Service Desk Management, Technology and People.

4.6   Service Desk Management

The Service Desk is the primary point of contact for users when there is an IT service disruption or request for change. The Service Desk provides a point of communication to the users and a point of coordination for several IT groups and processes.

There are a number of key IT Operations processes that must link together to provide an effective overall Service Desk. These include Incident Management, Event Management and Problem Management.

4.7   IT Continuity Management

As technology is a core component of most business processes, continuity or high availability of IT services is critical to the survival of the business as a whole. This is achieved by introducing risk reduction measures and recovery options. The purpose of ITCM is to maintain the necessary ongoing recovery capability within the IT services and their supporting components.

IT division develops and maintain IT Disaster Recovery Plan in accordance with the approved Bank's business impact analysis, business continuity plan and requirements.

5   IT Security

5.1   Objective and Overview

IT Security is dealing with the Bank's informational assets in electronic form and is a component of the Information Security framework, defined in the NDB Information Security Policy, to be approved by the NDB BoD, which provides the Bank with strategic direction for informational assets security activities and ensures objectives are achieved.

The Bank should ensure the security of IT systems and digital informational assets is adequately managed, ensure the continuity of business activities, and ensure the confidentiality, completeness and availability of business critical information.

IT Security requirements are defined in the NDB IT Security Standard, as a supplementary document to IT Policy, to be reviewed by the Chief of IT on a periodic basis to ensure it continues to be relevant and achieves its objective of servicing the wider organization.

5.2   IT Change Risk Management

IT division should assess the security of the existing IT landscape, as well as, the IT Security impact of planned IT system changes.

If there is any issue and/or impact, an IT security risk evaluation must be conducted in accordance with IT Service Management Policy and supplementary Standards to ensure whether any additional security control is required.

5.3   NDB Customer Information Protection

The Bank should place emphasis on the security of NDB customer information and other business information.

IT and other divisions/functions should develop and maintain guidelines and procedures in compliance with Information Security Policy and take effective actions to ensure the security of the Bank's business and customer information, which is stored electronically.

5.4   Identity & Access Management

IT Access Management is the process of granting authorized users the right to use an IT service, while preventing access to non-authorized users.

IT Access Management provides the right for users to be able to use an IT service or group of services.

5.5   Awareness of IT Security

IT should provide necessary IT Security related training and educational awareness to all NDB staff.

All contracts, signed by the Bank and its vendors, should include confidentiality and integrity requirements, and specify their IT security obligations and responsibilities towards each other.

The Bank may execute a third party security review or application security risk assessment, where necessary.

5.6   IT Audit

All IT processes must be compliant with the NDB IT policies, approved by the NDB BoD, and supplementary IT standards.

The Bank should conduct internal IT audit on a regular basis in order to assess the compliance of IT processes, required for the implementation and operation of the critical IT systems and/or services.

Management must take appropriate action in response to NDB internal auditors' recommendations and the relevant IT compliance model must be followed.