NORGES BANK
INVESTMENT MANAGEMENT

POLICY

INFORMATION TECHNOLOGY (IT)

Issued by	Chief Executive Officer
Issued	20/03/2012
Updated	14/01/2019

1. Purpose

This policy defines principles for delivery of information through systems, services and technology. The objective is to ensure a common set of principles, requirements and expectations to govern the information technology capabilities of the organisation and the relationship between consumers and providers of such capabilities.

This policy is based on NBIM Policy Management Framework and Financial Reporting and the COBIT good practice framework for information and technology governance, adapted to our operational model for IT services. It is divided in four main IT governance areas. Plan and organise (2.1 to 2.5), Build, acquire and implement (2.6 to 2.8), Deliver and support (2.9 to 2.13), and Monitor and evaluate (2.14).

2. Policy

Information Technology (IT) is in this policy referred to as data, systems, services and technologies that together provides Norges Bank Investment Management (NBIM) with information, electronic communication and efficient business process execution capabilities.

2.1 Strategy and technology direction

- The information technology strategy shall describe strategic objectives, tactical plans and direction for information technology, security, solutions and services. It shall also provide an evaluation of current information technology risks, performance and contribution.
- The information technology strategy shall have its foundation in the overall strategy plan.
- Technology direction shall ensure standardisation and consolidation of solutions and technologies.
- NBIM will foster business innovation by actively pursuing opportunities enabled by emerging technologies.

2.2 Architecture

- Information architecture, solution architecture, security architecture and technology architecture are part of the overall architecture represented in NBIM's Management Framework.
- An overview of the current state architecture shall be available at all times.

- Architecture compliance for new and existing solutions and technology shall be defined through principles with a foundation in this policy, strategy and technology direction.

2.3 IT processes, organisation and relationships

- IT processes, organisation and relationships are defined as part of the Management Framework.
- All information technology processes shall be assessed for quality and compliance with control requirements.

2.4 Operational risk, quality assurance and security

- Assessment and handling of operational risk is governed on an organisation level, across IT and other processes, in accordance with the operational risk framework.
- All solutions shall have a set of business criticaility and information security requirements that are monitored and optimised regularly.

2.5 IT projects

- Major changes to architecture and solutions shall be implemented through projects. All projects shall have a foundation in the overall strategy plan.
- Governance and the management of projects should be in accordance with methodology set out in internal guidelines.

2.6 Onboarding and offboarding of solutions

- Identification and procurement of new solutions shall follow general procurement rules in accordance with defined procurement processes.
- Business requirements and business case evaluation shall be the basis of acquiring or developing solutions.
- Technology choices shall be based on solution requirements and technology direction.
- NBIM has a preference to purchase commercial services over building these ourselves.
- An onboarding process shall be in place to ensure that architectural, security, quality and operational aspects are considered for all new solutions.
- An offboarding process shall be in place to ensure safe disposal of data and technology assets.

2.7 Development

- Solutions development, configuration and maintenance shall follow defined development and coding standards.
- We shall encourage distributed solution development to enable implementation of innovative and differentiating ideas in support of core activities.
- Different development methodologies and governance requirements are applied depending on a solution’s maturity, level of innovation and acceptable risk.

2.8 IT change management

- All changes within the production environment shall be managed through a risk based change management process.

- The change management process shall cover release and deployment, change, configuration, validation and testing as well as change assessment.

2.9 Service level management

- An overview of services and solutions shall be maintained. The overview shall include service definitions, service levels, criticality classification, solution ownership and responsibility.
- Services shall be cost efficient. A cost picture including direct and indirect cost shall be maintained for all services. All costs should be followed up on a regular basis in accordance with NBIM Policy Management Framework and Financial Reporting.

2.10 Systems management

- All systems shall have a system owner which represents the business areas drawing benefits from the system.
- All systems shall have a system manager who supports the system owner as required, and ensures that necessary support, change, control and training processes are in place.
- Provider management shall follow general rules in accordance with service provider management principles.

2.11 Data management

- We shall ensure cost-efficient provisioning of data.
- Management of data shall be prioritised according to business value and materiality.
- Data and information elements shall be defined and classified in a central repository.

2.12 Service request, incident and problem management

- NBIM shall have timely and effective processes to handle incidents and service requests.
- Root cause analysis shall be done for high impact incidents.

2.13 IT security and business continuity

- IT security and business continuity shall ensure integrity of information and protect information and IT infrastructure to minimise business impact of security vulnerabilities and incidents.
- IT security measures shall take into account confidentiality, integrity and availability classifications of the solutions and data to be protected.
- Disaster recovery for information systems and services shall follow general business continuity management processes.
- IT disaster recovery procedures shall be established and tested on a regular basis.

2.14 Monitor and evaluate

- Reporting shall ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels in accordance with requirements.
- Reporting shall be based on agreed upon targets for processes and performance.

- Reporting shall be balanced between service level improvement opportunity and reporting effort.