Ringkasan Kebijakan Umum Teknologi Informasi

PT Bank JTrust Indonesia Tbk

Overview of Information Technology General Policy

PT Bank JTrust Indonesia Tbk

A. Tata Kelola Teknologi Informasi

Sejalan dengan Surat Edaran Otoritas Jasa Keuangan nomor 21/SEOJK.03/2017 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum, PT Bank JTrust Indonesia Tbk memiliki Kebijakan Umum Teknologi Informasi. Kebijakan tersebut bertujuan memberikan arahan dan pengendalian untuk melaksanakan proses-proses teknologi informasi bank guna mencapai keselarasan yang tinggi antara arahan perkembangan dan kapabilitas teknologi informasi. Kebijakan Umum Teknologi Informasi ditinjau dan diperbarui setiap 2 (dua) tahun dengan pembaruan terakhir pada Juli 2023. Kebijakan umum TI mengatur beberapa ketentuan diantaranya:

1. Kebijakan Manajemen TI;
2. Kebijakan Tata Kelola TI;
3. Kebijakan Arsitektur TI, Perencanaan Strategis dan Penyusunan Anggaran TI;
4. Kebijakan Manajemen Risiko TI;
5. Kebijakan Pengembangan dan Pengadaan TI;
6. Kebijakan Perancangan dan Pengembangan Layanan TI;
7. Kebijakan Manajemen Proyek TI;
8. Kebijakan Pengadaan TI;
9. Kebijakan Operasional TI;
10. Kebijakan Kegiatan Operasional Layanan TI;
11. Kebijakan Dukungan Layanan TI;
12. Kebijakan Pemantauan dan Evaluasi Layanan TI;
13. Kebijakan Jaringan Komunikasi;
14. Kebijakan Pengamanan Infomasi, Ketahanan dan Keamanan Siber;
15. Kebijakan Rencana Pemulihan Bencana; dan
16. Kebijakan Layanan Perbankan Elektronik.

A. Information Technology Governance

In line with the Financial Services Authority Circular Letter No. 21/SEOJK.03/2017 regarding implementation of risk management in the use of information technology by commercial banks, PT Bank JTrust Indonesia Tbk has an Information Technology general policy. This policy aim to be a guidance for implementation of information technology processes in order to harmonize the directions of IT development with IT capabilities. This policy is reviewed and updated every 2 (two) years with the last update on July 2023. IT general policy regulate several provisions:

1. *IT Management Policy;*
2. *IT Governance Policy;*
3. *IT Architechture, Strategic Plan, and Budgeting Policy;*
4. *IT Risk Management Policy;*
5. *IT Development and Procurement Policy;*
6. *IT Planning and Development Policy;*
7. *IT Project Management Policy;*
8. *IT Procurement Policy;*
9. *IT Operation Policy;*
10. *IT Operational Services Policy;*
11. *IT Support Services Policy;*
12. *IT Monitoring and Evaluation Policy;*
13. *Communication Network Policy;*
14. *Information Security, Cyber Security and Resiliency Policy;*
15. *Disaster Recovery Policy; and*
16. *Electronic Banking Services Policy.*

Penerapan tata kelola TI yang baik berlaku bagi seluruh unit dan/atau fungsi pengelola TI dan pengguna TI. Kegiatan-kegiatan yang harus dilakukan dalam penerapan Tata Kelola TI meliputi:

1) Evaluasi atas pilihan strategi, pengarahan atas strategi penyelenggaraan TI, dan pemantauan pencapaian strategi;
2) Penyelarasan, perencanaan, dan pengorganisasian seluruh unit, strategi, dan kegiatan yang mendukung penyelenggaraan TI;
3) Pendefinisian, akuisisi, dan implementasi atas solusi TI serta integrasinya dalam proses bisnis Bank;
4) Penyediaan dukungan operasional layanan TI kepada pemangku kepentingan; dan
5) Pemantauan kinerja dan kesesuaian penyelenggaraan TI dengan target kinerja intern, pengendalian intern, dan ketentuan peraturan perundang-undangan.

Good IT Governance is applied to all unit and/or IT controlling function and users. Activities that must be carried out in the implementation of IT Governance:

1) Evaluation of strategy options, strategy implementations, and strategy achievement monitoring;
2) Harmonization, planning, and organizing all unit, strategy, and activity that support IT performance;
3) Defining, acquisition, and implementation of IT solutions and their integration into the Bank's business processes;
4) Provision of IT operational support to the stakeholder; and
5) Monitor the performance and compliance of IT implementation with internal performance targets, internal controls, and regulatory provisions.

B. Manajemen Risiko TI

Manajemen risiko TI tertuang dalam prosedur standar operasional (SOP) serta *Working Instruction* yang berlaku di bank sebagai komitmen pengendalian risiko TI.

1. Tujuan

Kebijakan Manajemen Risiko TI bertujuan menjadi pedoman pengendalian risiko TI demi memastikan kelangsungan dan meningkatkan kualitas layanan yang lebih baik sehingga dapat memberikan layanan inovatif terbaik kepada pemegang kepentingan (*stakeholders*) Bank.

2. Kebijakan Umum

a. Proses pengelolaan risiko TI dilakukan sesuai dengan kerangka kerja manajemen risiko Bank.
b. Manajemen TI menentukan penanganan risiko TI beserta prioritasnya berdasarkan *risk appetite* TI dan pertimbangan bisnis.

B. IT Risk Management

IT risk management listed on Standard Operational Procedure and Working Instruction that apply in bank as a commitment of IT risk control.

1. Objective

IT Risk Management policy aim to be a guidance for IT risk management in order to ensure the continuity and upgrade the service quality so can deliver the best inovative services to the stakeholders.

2. General Policy

a. The IT risk management process is carried out in accordance with the Bank's risk management framework.
b. IT management determines IT risk management and its priorities based on IT risk appetite and business considerations.

c. Divisi Teknologi Informasi menempatkan *risk appetite*-nya sesuai dengan kebijakan strategis Bank.
d. Penanganan risiko TI dengan eksposur tinggi menjadi prioritas utama Manajemen TI dan dilaksanakan segera.
e. Proses manajemen risiko terkait teknologi informasi harus dilakukan secara terintegrasi dalam setiap tahapan penyelenggaraan TI, dengan proses paling sedikit:
   1) Identifikasi risiko.
   2) Pengukuran risiko.
   3) Pemantauan risiko.
   4) Pengendalian risiko.

3. Identifikasi dan Pengukuran Risiko TI

a. Sesuai dengan koordinasi dengan Manajemen unit kerja Manajemen Risiko Bank, unit kerja dan manajemen TI mengidentifikasi risiko TI baik yang telah ada maupun risiko-risiko baru yang muncul akibat perubahan dan dituangkan ke dalam *Risk Register*.
b. Manajemen TI menentukan penanganan risiko dengan menerima (*accept*), menghindari (*avoid*), mengalihkan (*transfer*) atau mengendalikan (*mitigate*) risiko tersebut.

4. Pemantauan dan Pelaporan Risiko TI

a. Meminta *Risk taking unit* untuk melaporkan status mitigasi risiko pada Manajemen TI dan unit kerja Manajemen Risiko Bank secara berkala.
b. Manajemen TI dan unit kerja Manajemen Risiko Bank memastikan *risk taking unit* melakukan langkah-langkah mitigasi risiko.

5. Pengendalian Risiko TI

Risk taking unit melakukan langkah-langkah mitigasi risiko yang telah ditentukan oleh Manajemen Bank.

C. Manajemen Pengamanan Informasi TI

Bank juga berkomitmen untuk menjaga keamanan informasi, kerahasiaan, integritas dan ketersediaan informasi dan infrastruktur TI. Komitmen tersebut diwujudkan melalui implementasi kebijakan, rencana dan prosedur

c. The Information Technology Division places its risk appetite in accordance with the Bank's strategic policies.
d. Handling IT risks with high exposure is a top priority for IT Management and will be implemented immediately.
e. The risk management process related to information technology must be carried out in an integrated manner in every stage of IT implementation, with at least the following processes:
   1) Risk identification.
   2) Risk measurement.
   3) Risk monitoring.
   4) *Risk control*

3. Identification and Risk Measurement

a. In accordance with the coordination with the Management of the Bank's Risk Management work unit, the work unit and IT management identify existing IT risks as well as new risks that arise as a result of changes and are poured into the Risk Register.
b. IT management determines how to handle risks by accepting, avoiding, transferring or mitigating those risks.

4. IT Risk Monitoring and Reporting

a. Ask Risk taking unit to report risk mitigation status to IT managementt and Risk Management unit regularly
b. IT Management and bank risk management unit ensure that risk taking unit take risk mitigation action.

5. IT Risk Control

The risk taking unit carries out risk mitigation measures that have been determined by the Bank's Management.

C. IT Information Security Management

Bank also committed to ensure the security, secrecy, integrity and availability information and IT infrastructure. That commitment embodied by the implementation of information securitty policies, plans and procedures, as well

pengamanan informasi serta aktivitas pemantauan, deteksi, pelaporan dan tindak lanjut atas insiden keamanan dan laporan kelemahan keamanan.

Divisi TI berperan sebagai koordinator utama dari upaya-upaya pengamanan layanan TI dengan melakukan:

1) Pengendalian terhadap *malicious code;*
2) Menjamin ketersediaan data dan kemampuan pemulihan sistem;
3) Mengkoordinasikan implementasi pengendalian untuk mengamankan jaringan komunikasi data; dan
4) Membatasi akses terhadap layanan TI dan komponen pendukungnya sesuai kebutuhan Bank.

D. Rencana Pemulihan Bencana TI

Dalam keadaan darurat atau bencana, manajemen TI memiliki kebijakan guna menjaga dan memulihkan layanan TI dengan menerapkan rencana pemulihan bencana (*disaster recovery)* sesuai kebutuhan. Prosedur *Disaster Recovery Plan* TI Bank diselaraskan kepada prosedur *Business Continuity Plan*. Manajemen menetapkan pilihan dan strategi pemulihan berdasarkan hasil *Business Impact Analysis* dan hasil analisa risiko. Manajemen menetapkan struktur organisasi dan anggota tim *Disaster Recovery* yang diperbaharui setiap tahunnya. Prosedur *Disaster Recovery Plan* diperbaharui agar selalu mencerminkan kondisi terkini.

as monitoring, detecting, reporting, and following-up activities on seccurity incidents and security flaw report.

The IT Division serves as the main coordinator for efforts to secure IT services ad perfforms:

a) Control ontrol over malicious code;
b) Ensure data availability and system recovery capabilities;
c) Coordinate the implementation of controls to secure data communication networks; and
d) Limiting access to IT services and supporting components according to the needs of the Bank.

D. IT Disaster Recovery Plan

In a state of disaster or emergency, IT management has policy to protect and recover IT service by implementing IT Disaster Recovery Plan according to the needs. IT Disaster Recovery Plan Procedure aligned with Business Continuity Plan procedure. Management assign options and recovery strategy based on the result of Business Impact Analysis and the result of risk analysis. Management set the organization structure and team member of Disaster Recovery that updatetd every year. Disaster Recovery Plan updated to always reflect current conditions.