Bank Resona Perdania

KEBIJAKAN PENGAMANAN INFORMASI DAN MANAJEMEN RISIKO SISTEM DALAM PENGGUNAAN TEKNOLOGI INFORMASI

INFORMATION SECURITY AND SYSTEM RISK MANAGEMENT POLICY IN THE USE OF INFORMATION TECHNOLOGY

Edisi ke-7, September 2022

7th Edition, September 2022

BOD Approval No. 256/ITD/IT-Ops/X/2022

BOC Approval No. 164/BOC/X/2022-ITD/IT-OPS

DAFTAR ISI
Table of Content

Bank Resona Perdania

I. PENDAHULUAN

A. Latar Belakang

Informasi adalah aset yang sangat penting bagi Bank, baik informasi yang terkait dengan nasabah, keuangan, laporan maupun informasi lainnya. Kebocoran, kerusakan, ketidakakuratan, ketidaktersediaan atau gangguan lain terhadap informasi tersebut dapat menimbulkan dampak yang merugikan baik secara finansial maupun non-finansial bagi Bank. Dampak dimaksud tidak hanya terbatas pada Bank tersebut, namun juga nasabah, Bank lain dan bahkan terhadap sistem perbankan nasional. Mengingat pentingnya informasi, maka informasi harus dilindungi atau diamankan oleh seluruh personil di Bank.

B. Acuan

1. Undang-Undang Republik Indonesia (UU RI) No.7 Tahun 1992 sebagaimana telah diubah dengan UU RI No.10 Tahun 1998 tentang Perbankan;

2. UU RI No.11 Tahun 2008 sebagaimana telah diubah dengan UU RI No.19 Tahun 2016 tentang Informasi dan Transaksi Elektronik;

3. Peraturan Pemerintah Republik Indonesia No.71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;

4. Peraturan Menteri Komunikasi dan Informatika Republika Indonesia No.5 Tahun 2020 tentang Penyelenggaraan Sistem Elektronik Lingkup Privat ;

5. Peraturan Menteri Komunikasi dan Informatika Republika Indonesia No.20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik;

I. INTRODUCTION

A. Background

Information is a very important asset for Banks, one related to customers, finance, report or other information. Leakage, damage, inaccuracy, unavailability or other disturbances on information can cause both financial and non-financial losses for Banks. Those effects are not only limited to the Bank, but also to customers, other Banks and even to national banking systems. Considering the importance of information, it must be protected or secured by the entire personnel in a Bank.

B. Reference

1. Law of the Republic of Indonesia (UU RI) No. 7 of 1992 as amended by Law of the Republic of Indonesia No. 10 of 1998 about Banking;

2. The Law of the Republic of Indonesia No.11 of 2008 as amended by Law of the Republic of Indonesia No.19 of 2016 concerning Information and Electronic Transactions;

3. Government Regulation of the Republic of Indonesia No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions;

4. Regulation of the Minister of Communication and Information of the Republic of Indonesia No. 5 of 2020 concerning the Implementation of Private Electronic Systems ;

5. Regulation of the Minister of Communication and Information of the Republic of Indonesia No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems;

6. POJK No.38/POJK.03/2016 sebagaimana telah diubah dengan POJK No.13/POJK.03/2020 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum;

   Sejak 30 Okt 2021 Pasal 30 ayat (3) dan ayat (4) POJK Nomor 38 /POJK.03/2016 tentang penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum sepanjang berkaitan dengan perubahan laporan rencana pengembangan teknologi informasi atas rencana penyelenggaraaan Produk Bank lanjutan berupa kegiatan berbasis teknologi informasi, dinyatakan dicabut dan tidak berlaku oleh POJK No.13/POJK.03/2021 tentang Penyelenggaraan Produk Bank Umum;

   Sejak 7 Oktober 2022 POJK No.28/POJK.03/2016, POJK No.13/POJK.03/2020 di cabut oleh No.11/POJK.03/2022;

6. POJK No.38/POJK.03/2016 as amended by POJK No.13/POJK.03/2020 concerning the Implementation of Risk Management in the Use of Information Technology by Public Banks;

   Since October 30, 2021 Article 30 paragraph (3) and paragraph (4) of POJK Number 38 /POJK.03/2016 concerning the application of Risk Management in the Use of Information Technology by Commercial Banks as long as it relates to changes in the information technology development plan report on the plan for the implementation of further Bank Products in the form of information technology-based activities, declared revoked and invalid by POJK No.13/POJK.03/2021 concerning the Operation of Public Bank Products;

   Since October 7, 2022 POJK No.28/POJK.03/2016, POJK No.13/POJK.03/2020 has been revoked by No.11/POJK.03/2022

7. SEOJK No.21/POJK.03/2017 tanggal 6 Juni 2017 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum;

   SEOJK No.21/POJK.03/2017 ini dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam POJK No.11/POJK.03/2022

8. POJK No.11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum (berlaku sejak 7 Oktober 2022);

9. POJK No.18/SEOJK.03/2016 tentang Penyelenggaraan Manajemen Risiko Bagi Bank Umum;

   Sejak 30 Okt 2021, Pasal 20, Pasal 21, Pasal 22 dan Pasal 24 dalam POJK No.18/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum dinyatakan di cabut dan tidak berlaku oleh POJK No.13/POJK.03/2021 tentang Penyelenggaraan Produk Bank Umum;

7. SEOJK No. 21/POJK.03/2017 dated June 06, 2017 about Implementation of Risk Management in used Information Technology by public Bank;

   SEOJK No.21/POJK.03/2017 is declared still valid as long as it does not conflict with the provisions in POJK No.11/POJK.03/2022

8. POJK No.11/POJK.03/2022 concerning Implementation of Information Technology by Public Banks (effective since October 7, 2022);

9. POJK No.18/SEOJK.03/2016 concerning Implementation of Risk Management for Public Banks;

   Since October 30, 2021, Article 20, Article 21, Article 22 and Article 24 in POJK No.18/POJK.03/2016 concerning Implementation of Risk Management for Public Banks are declared to be revoked and invalid by POJK No.13/POJK.03/2021 concerning Implementation Public Bank Products;

10. SEOJK No.34/SEOJK.03/2016 tanggal 1 September 2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum.

11. PADG No.23 /25/PADG/2021 tanggal 12 November 2021 tentang Penyelenggaraan BI-Fast Payment;

12. PADG No.23/19/PADG/2021 tanggal sejak 13 September 2021 tentang penyelenggaraan Aplikasi Layanan Bank Indonesia;

    Pada saat PADG ini berlaku, SEBI No.18 tanggal 28 Januari 2016 perihal Penyelenggaraan Sistem BI Government Electronic Banking di cabut dan dinyatakan tidak berlaku;

13. POJK No.6/POJK.07/2022 tanggal 18 April 2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa keuangan;

14. Kebijakan Manajemen Risiko Secara Umum (Individual);

15. Kebijakan Manajemen Risiko Teknologi Informasi;

16. Kebijakan Manajemen Risiko Operasional.

17. Kebijakan Pengawasan Keamanan Sistem dan Informasi.

18. Kebijakan Audit Intern Teknologi Informasi.

19. Kebijakan Manajemen Proyek dan Pengembangan Sistem.

20. Kebijakan Penyimpanan Dokumen Perusahaan.

21. Kebijakan Tugas dan Wewenang;

22. Kebijakan Job Description.

10. SEOJK No.34/SEOJK.03/2016 dated September 1, 2016 concerning the Implementation of Risk Management for Public Bank;

11. PADG No.23/25/PADG/2021 dated 12 November 2021 concerning the Implementation of BI-Fast Payment;

12. PADG No.23/19/PADG/2021 dated September 13, 2021 regarding the implementation of Bank Indonesia Service Applications;

    At the time this PADG comes into effect, SEBI No.18 dated January 28, 2016 regarding the Implementation of the BI Government Electronic Banking System is revoked and declared invalid;

13. POJK No.6/POJK.07/2022 dated 18 April 2022 concerning Consumer and Community Protection in the Financial Services Sector;

14. General Risk Management Policy (Individual);

15. Information Technology Risk Management Policy;

16. Operational Risk Management Policy;

17. System and Information Security Monitoring Policy;

18. Information Technology Internal Audit Policy;

19. Project Management and System Development Policy;

20. The Corporate Document Retention Policy;

21. Duties and Authorities Policy;

22. Job Description Policy.

C. Tujuan

Dalam upaya melakukan pencegahan atas timbulnya kerugian akibat risiko penggunaan teknologi terkait informasi, Bank Resona Perdania (selanjutnya disebut “Bank”) membuat "Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem Dalam Penggunaan Teknologi Informasi".

C. Purpose

In effort to prevent loss from risk of using technology related to information, Bank Resona Perdania (hereinafter refer as "Bank") establish "Information Security and System Risk Management Policy in the use of Information Technology".

II. TUGAS DAN TANGGUNG JAWAB

A. Dewan Komisaris

1. Mengevaluasi, mengarahkan dan memantau rencana strategis teknologi informasi dan kebijakan bank terkait penggunaan teknologi Informasi.

2. Mengevaluasi pertanggung jawaban Direksi atas penerapan manajemen risiko dalam penggunaan Teknologi Informasi.

B. Komite Pengarah Teknologi Informasi

Komite Pengarah Teknologi Informasi bertanggung jawab untuk memberikan rekomendasi kepada Direksi paling sedikit terkait dengan :

1. Rencana strategis Teknologi Informasi yang sejalan dengan rencana strategis kegiatan usaha Bank;

2. Perumusan kebijakan, standar, dan prosedur Teknologi Informasi yang utama;

3. Kesesuaian antara proyek Teknologi Informasi yang disetujui dengan Rencana Startegis Teknologi Informasi;

4. Kesesuaian antara pelaksanaan proyek Teknologi Informasi dengan rencana proyek yang di sepakati (*project charter*);

5. Kesesuaian antara Teknologi Informasi dengan kebutuhan sistem Informasi manajemen serta kebutuhan kegiatan usaha Bank;

6. Efektifitas langkah-langkah dalam meminimalkan risiko atas investasi Bank pada sektor Teknologi Informasi agar investasi Bank pada sektor Teknologi Informasi memberikan kontribusi terhadap pencapaian tujuan bisnis Bank;

7. Pemantauan atas kinerja Teknologi Informasi dan upaya peningkatan kinerja Teknologi Informasi;

II. JOB AND RESPONSIBILITY

A. Board of Commissioners

1. Evaluated, directed and monitor information technology and bank policies related to use information technology.

2. Evaluating Board of Director responsibility of implementationof risk management in use Information Technology.

B. IT Steering Committee

IT Steering Committee is responsible to presenting recommendations to the Board of Directors which at least regarding:

1. Information technology strategic plan in line with strategic bussines bank;

2. Policy Formulation, standard and main information technology procedure;

3. Compatibility between information technology projec approved with Information Technology strategic plan;

4. Compatibility between information technology project implementation with Information Technology plan (project charter);
.

5. Compatibility between information technology with management information system needs and then business bank activites;

6. Effectiveness of steps for minimilized risk for bank invesment in information technology sector so that bank investment in information technology sector contribute to achievement business bank purpose;

7. Monitoring performance of information technology and effort to improve information technology;

8. Upaya penyelesaian berbagai masalah terkait Teknologi Informasi secara efektif, efisien dan tepat waktu;

9. Kecukupan dan alokasi sumber daya yang dimiliki Bank;

C. Direksi

1. Menetapkan Rencana Strategi Teknologi Informasi dan kebijakan Bank terkait penggunaan Teknologi Informasi;

2. Menetapkan kebijakan, standar, dan prosedur terkait penyelenggaraan Teknologi Informasi yang memadai dan mengomunikasikannya secara efektif, baik pada satuan kerja penyelenggara maupun pengguna Teknologi Informasi;

3. Memastikan :

   3.1 Teknologi Informasi yang digunakan Bank dapat mendukung perkembangan usaha, pencapaian tujuan bisnis dan kelangsungan pelayanan terhadap nasabah

   3.2 Terdapat kegiatan peningkatan kompetensi sumber daya manusia yang terkait dengan penyelenggaraan dan penggunaan Teknologi Informasi

   3.3 Ketersediaan sistem pengelolaan pengamanan informasi *(Information Security Management System)* yang efektif dan dikomunikasikan kepada satuan kerja pengguna dan penyelenggaraan Teknologi Informasi

   3.4 Penerapan Proses Manajemen Risiko dalam penggunaan Teknologi informasi dilaksanakan secara memadai dan efektif

   3.5 Kebijakan, standar dan prosedur Teknologi Informasi di terapkan secara efektif pada satuan kerja pengguna

8. Effort to solve any problem related information technology with effective, efficient dan on time;

9. Adecuacy and allocation of resource owned by bank;

C. Board of Directors

1. Establish information technology strategic plan and bank policies related to use information technology;

2. Establish policies, standard and procedure related implementation of information technology and communicate it effectively, both in work unit and user of information technology;

3. Ensure :

   3.1 Information technology used by bank can support business bank and achievement bank purpose and continuity

   3.2 There are activities to improve competency of human resource related about implementation and used Information Technology

   3.3 Availibility of Information Security Management System effectively and communicated user in working unit and implementation of information technology

   3.4 Risk Management Proces implementation use in information technology held adequately and effectively

   3.5 Information technology policies, standard and procedure effectively applied to working unit user and

dan penyelenggara Teknologi Informasi

3.6 Terdapat sistem pengukuran kinerja proses penyelenggaraan Teknologi Informasi yang paling sedikit dapat:

a. Mendukung proses pemantauan terhadap implementasi strategi

b. Mendukung penyelesaian proyek pengembangan Teknologi Informasi

c. Mengoptimalkan pendayagunaan sumber daya manusia dan investasi pada infrastruktur

d. Meningkatkan kinerja proses penyelenggaraan Teknologi Informasidan kualitas layanan penyampaiaan hasil proses kepada pengguna Teknologi informasi.

information technology provider

3.6 There is information technology performance measurement system at least :

a. Support monitoring process for implementation startegy

b. Support completion of information technology development project

c. Optimizing the utilization of human resource and investment in infrastructure

d. Improve performance process information technology nad service quality delivery process result to information technology users.

D. Kepala Divisi Teknologi Informasi

1. Mengevaluasi, mengarahkan dan memantau penggunaan teknologi informasi terkait prosedur Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem Dalam Penggunaan Teknologi Informasi.

2. Mengevaluasi pertanggung jawaban divisi TI atas penerapan manajemen risiko dalam penggunaan teknologi informasi terkait Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem Dalam Penggunaan Teknologi Informasi.

D. Head Of Information Technology

1. Evaluated, directed and monitoring the use of information technology in relation to Information Security and System Risk Management Policy In The Use Of Information Technology procedures.

2. Evaluating the accountability of the IT division for the implementation of risk management in the use of information technology related to Information Security and System Risk Management Policy In The Use Of Information Technology procedures.

E. Seksi Keamanan Informasi dan Risiko Sistem

1. Pengelolaan fungsi pengamanan informasi agar sesuai dengan kebijakan dan ketentuan serta *best practice* yang berlaku.

2. Pemantauan sistem administrator, data administrator, jaringan administrator dan pelaksanaan pengamanan informasi di setiap Divisi atau satuan kerja.

3. Mengkomunikasikan dan mengajarkan program pengamanan informasi termasuk melakukan upaya peningkatan kesadaran akan pengamanan (*security awareness program*) kepada staf / karyawan.

4. Menetapkan kriteria dan definisi pengukuran risiko pengamanan informasi.

5. Melaksanakan program penilaian risiko pengamanan informasi termasuk menilai kepatuhan seluruh Divisi terhadap kebijakan pengamanan informasi dan merekomendasikan pengendalian yang perlu dilakukan.

6. Memastikan pihak ketiga yang memiliki akses terhadap informasi rahasia milik Bank telah menerapkan pengamanan informasi secara memadai dan konsisten.

7. Membantu koordinasi pengujian BCP.

8. Melaporkan kepada Direktur terkait jika terdapat gangguan, masalah, kejahatan terkait pengamanan informasi.

9. Mengawasi pemeliharaan sistem dan rencana perbaikan manajemen risiko sistem.

E. Information Security and System Risk Section

1. The management of information security functions to be in accordance with valid policies and regulations as well as valid best practices.

2. Monitoring the system administrator, data administrator, network administrator and information security implementation in every Division or work unit.

3. Communicating and educate employee include implementation effort of information security program to increase awareness on security (security awareness program)to staf / employee.

4. Determining the criteria and definition of information security risk measurement.

5. Carrying out information security risk assessment including assessing the compliance of each and every division in a Bank on information security, and recommending necessary control.

6. Ensuring that a third party with authorization to a Bank’s confidential information has implemented information security adequately and consistently.

7. Assisting the coordination of BCP testing.

8. Report to related Director, if there is any disruption, problem, crime related to information security.

9. Supervising system maintenance and improvement plan of system risk management.

F. Seksi Perencanaan TI dan Fungsi Operasional dan Dukungan TI

1. Menentukan prosedur manajemen sistem dan menerapkan sistem pengamanan untuk memastikan kelancaran sistem dan mencegah penipuan.
2. Melakukan pemeriksaan sistem aset secara berkala.
3. Mengelola penggunaan komputer di internal atau komputer yang digunakan untuk keperluan di eksternal Bank.
4. Memastikan kerahasiaan, ketersediaan, integritas, keaslian dan *non repudiation* data.
5. Menentukan prosedur manajemen data dan prosedur pengelolaan data untuk penggunaan internal dan eksternal.
6. Mengelola perlindungan data dan pencegahan terkait akses data yang tidak sah.
7. Mengelola dan memantau jaringan operasional dan kontrol akses.
8. Menentukan prosedur manajemen jaringan dan prosedur penggunaan jaringan untuk internal dan eksternal.
9. Melakukan kajian terkait prosedur jaringan *backup*.
10. Melakukan tinjauan atas risiko sistem yang mengacu kepada Kebijakan Manajemen Risiko Teknologi Informasi.
11. Membuat pedoman terkait kegagalan sistem dan pengamanan informasi yang tercakup dalam rencana keberlangsungan sistem.

F. IT Planning Section and IT Support and Operational Function

1. Specify system management procedure and apply a safety and smooth system and prevent fraud.
2. Perform system assets examination on regular basis.
3. Manage internal use of computer or computer which being used for usage at external Bank.
4. Ensure the data confidentiality, availability, integrity, authenticity and non repudiation.
5. Specify data management procedure and manage data usage procedure for internal and external parties.
6. Manage data protection and prevention of unauthorized data access.
7. Manage and monitoring network operation and access control.
8. Specify network management procedure and usage procedure for internal and external parties.
9. Consider backup network procedure.
10. Conduct review of system risk register that refer to Risk Management Policy of Information Technology.
11. Create guideline about system failure and information security included in system contingency plan.

12. Membantu *user* bisnis dalam melakukan BCP yang mengacu pada Kebijakan *Business Continuity Plan* Sistem Operasional.

12. Assist business owner in performing BCP by refer to Business Continuity Plan of System Operational Policy.

G. Seksi Sistem TI dan Fungsi Proyek TI

1. Melakukan pelaporan berkala ke IT *Steering Committee* (mengacu kepada Kebijakan IT *Steering Committee*) mengenai status proyek pengembangan sistem yang penting atau sistem modifikasi dan status atas sistem terkait.
2. Mengembangkan standar metode pengembangan dan instalasi.
3. Melakukan pengukuran risiko atas pengembangan sistem baru atau sistem modifikasi.
4. Menentukan level kerahasiaan dan ketersediaan atas sistem baru atau modifikasi sistem.
5. Menentukan prosedur peralihan sistem selama proses pengembangan untuk memastikan pengamanan sistem produksi atas sistem baru atau modifikasi sistem.
6. Melaksanakan penilaian dan evaluasi sistem setelah proses peralihan sistem.
7. Rincian prosedur pengembangan sistem mengacu ke Kebijakan Manajemen Proyek dan Pengembangan Sistem.

G. IT System Section and IT Project Function

1. Conduct report on regular basis to IT Steering Committee (refer to IT Steering Committee Policy) about status of important system development project or modification of existing system and status of related system risk.
2. Develop standard of development method and installation.
3. Measure risk of new system development or modification of existing system.
4. Specify confidentiality level and availability level of new system or modification of existing system.
5. Specify switch over procedure to ensure the safety of production system during development of new system or modification of existing system.
6. Implement assessment and evaluation of the system after system switch over.
7. Details of system development procedure refer to Project Management and System Development Policy.

III. PRINSIP, KEBIJAKAN DAN PROSEDUR PENGAMANAN INFORMASI

A. Prinsip Pengamanan Informasi

Pengamanan informasi sekurang-kurangnya memperhatikan prinsip-prinsip sebagai berikut:

1. Dilaksanakan untuk meyakini bahwa informasi yang dikelola terjaga atas kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaannya (*availability*) secara efektif dan efisien dengan memperhatikan kepatuhan (*compliance*) terhadap ketentuan yang berlaku.
2. Memperhatikan aspek sumber daya manusia, proses dan teknologi.
3. Dilakukan berdasarkan hasil penilaian risiko (*risk assessment*) dengan memperhatikan strategi bisnis Bank dan ketentuan yang berlaku.
4. Menerapkan pengamanan informasi secara komprehensif dan berkesinambungan yaitu dengan menetapkan tujuan dan kebijakan pengamanan informasi, mengimplementasikan pengendalian pengamanan informasi, memantau dan mengevaluasi kinerja serta keefektifan kebijakan pengamanan informasi serta melakukan penyempurnaan.

B. Kebijakan Pengamanan Informasi

Kebijakan tentang pengamanan informasi mencakup sekurang-kurangnya:

1. Tujuan pengamanan informasi yang sekurang-kurangnya meliputi pengelolaan aset, sumber daya manusia, pengamanan fisik, pengamanan logic (*logical security*), pengamanan operasional TI, penanganan insiden pengamanan informasi, dan pengamanan informasi dalam pengembangan sistem.
2. Komitmen manajemen terhadap pengamanan informasi sejalan dengan strategi dan tujuan bisnis.

III. PRINCIPLES, POLICIES AND PROCEDURES OF INFORMATION SECURITY

A. Information Security Principles

Information security at least considers the following principles:

1. Ensure that the information being managed is secure by confidentiality, integrity, and availability in effective and efficient means by considering compliance to existing regulations.
2. Considers the aspect of human resources, process and technology.
3. Carried out based on the result of risk assessment with consideration to Bank's business strategy and existing regulations
4. Implement information security comprehensively and in continuity, by determining the purpose and policy of information security, by implementing information security control, monitoring and evaluating the performance as well as the effectiveness of information security policy, and by carrying out further refining.

B. Information Security Policy

Information security policy include at least:

1. The purpose of information security, which includes assets management, human resources, physical security, logical security, IT operation security, information security incidents response, and information security in system developments.
2. Management's commitment to securing information is in line with business strategies and objectives

3. Kerangka acuan dalam menetapkan pengendalian melalui pelaksanaan manajemen risiko Bank.

4. Kepatuhan terhadap ketentuan intern dan ketentuan peraturan perundang-undangan antara lain Undang-Undang mengenai informasi dan transaksi elektronik (UU ITE) dan peraturan pemerintah mengenai penyelenggaraan sistem dan transaksi elektronik (PP PSTE)

5. Pelatihan dan peningkatan kesadaran atas pentingnya pengamanan informasi (*security awareness program*)

6. Analisis dampak pengamanan informasi terhadap kelangsungan bisnis.

7. Tugas dan tanggung jawab pihak-pihak dalam pengamanan informasi

8. Prinsip dan standar pengamanan informasi, termasuk kepatuhan terhadap ketentuan yang berlaku, pelatihan dan peningkatan kesadaran atas pentingnya pengamanan informasi (*security awareness program*), rencana kelangsungan bisnis dan sanksi atas pelanggaran.

9. Dokumen atau ketentuan lain yang mendukung kebijakan pengamanan informasi.

C. Prosedur Pengamanan Informasi

1. Prosedur Pengelolaan Aset

a. Aset Bank yang terkait dengan informasi harus diidentifikasikan, ditentukan pemilik/penanggung jawawban dan dicatat agar dapat dilindungi secara tepat.

b. Aset yang terkait dengan informasi tersebut dapat berupa data (baik *hardcopy* maupun *softcopy*), perangkat lunak, perangkat keras, jaringan, peralatan pendukung (misalnya sumber daya listrik, *AC*) dan sumber daya manusia (termasuk kualifikasi dan keterampilan).

3. The framework of reference in establishing controls through the implementation of bank risk management.

4. Compliance with internal regulationand provision of legislation, among others, laws on information and electronic transaction (ITE Law) and government regulations regarding the implementation odf systems and electronic transactions (PP PSTE)

5. Training dan increasing awareness of the importance of information security (security awareness program)

6. Analysis of the impact of information security on business continuity.

7. Duties and responsibilities of parties in information security

8. Principles and standards of information security, including compliance to valid regulations, trainings and improvement of awareness on the importance of information security (security awareness program), business continuity plan and penalties on violation.

9. Documents or other regulations supporting the policies of information security.

C. Information Security Procedure

1. Asset Management Procedure

a. Bank’s assets related to information must be identified, its ownership decided and recorded so as to be properly protected.

b. Information asset can be in the form of data (hardcopy or softcopy), software, hardware, networks, supporting equipments (for example power source, AC) and human resources (including qualifications and skills).

c. Informasi perlu diklasifikasikan agar dapat dilakukan pengamanan yang memadai sesuai dengan klasifikasinya.

c. Information need to be classified for adequate security according to its classification.

1.1 **Klasifikasi Informasi**

1. Level Kerahasiaan

1.1 **Information Classification**

1. Confidentiality Level

Confidentiality Level	Information Classification	Target System
III	*Top Secret*	Sistem atau informasi yang memiliki kemungkinan untuk membuat dampak yang signifikan jika ada kebocoran, pengungkapan atau dipresentasikan. *System or information that has possibility to make a significant effect to environment if there is any leakage, disclosure or presented.* Orang yang bersangkutan dengan informasi tersebut yang menentukan bahwa informasi tersebut bersifat sangat rahasia dan tidak boleh digunakan oleh pihak lain kecuali internal pihak tersebut. *Person concerned in information decides that it is a top secret and shall not be used by other party except by themselves.*
II	*Secret*	Sistem atau informasi yang memiliki kemungkinan untuk membuat dampak yang signifikan jika ada kebocoran, pengungkapan atau dipresentasikan. *System or information that has possibility to make a significant effect to environment if there is any leakage, disclosure or presented.* Informasi ini tidak dapat digunakan oleh pihak lain kecuali oleh pihak terkait. *This information shall not be used by other party except its concerned party.*
I	*Limited within Bank*	Sistem atau informasi yang digunakan di dalam Bank untuk keperluan operasional, tetapi tidak dapat dibocorkan, diungkapkan atau dipresentasikan di luar Bank. *System or information that being used within Bank for work operation but shouldn't any leakage, disclosure or presented to outside of the Bank.*
-	*Unclassified*	Informasi yang dapat dipresentasikan di dalam Bank atau lingkungan tertentu dan informasi resmi Bank yang tidak dibatasi pengelolaannya. *Information that being presented within Bank or premises to be presented and official information that has no limitation to manage.*

2. Level Ketersediaan

2. Availability Level

Availability Level	***Target System***
Highest	Sistem yang perlu untuk diminimalkan tingkat kegagalannya terkait penyelesaian transaksi nasabah, jaringan dan lainnya. *System that need to minimize the failure in early stage about customer transaction settlement, network, etc.*
High	Sistem yang tidak memiliki dampak langsung pada operasional terkait nasabah atau sistem yang tidak memiliki limitasi atas jangkauan dampaknya. Sistem dengan klasifikasi ini digunakan dalam operasional Bank. *System that has no effect during work related with customer at any time or there is no limitation in its impact range. System that has advance priority in operational Bank.*
Middle	Sistem yang memiliki prioritas rendah terkait kegagalan sistem, pekerjaan tetap dapat dilakukan dengan proses manual. *System that has low priority of minimizing failure, continuation work based on manual operation.*
Unclassified	Sistem selain klasifikasi di atas. *System others than above.*

2. Prosedur Pengelolaan Sumber Daya Manusia

a. Sumber daya manusia baik Karyawan Bank, konsultan, dan Karyawan pihak penyedia jasa yang memiliki akses terhadap informasi harus memahami tanggung jawabnya terhadap pengamanan informasi.

b. Peran dan tanggung jawab sumber daya manusia baik Karyawan Bank, konsultan, dan Karyawan pihak penyedia jasa yang memiliki akses terhadap informasi harus didefinisikan dan didokumentasikan sesuai dengan kebijakan pengamanan informasi.

c. Dalam perjanjian atau kontrak dengan Karyawan Bank, konsultan, dan Karyawan pihak penyedia jasa harus tercantum ketentuan-ketentuan mengenai pengamanan Teknologi Informasi yang sesuai dengan kebijakan pengamanan informasi Bank.

2. Human Resource Management Procedure

a. Bank's employees, consultants, and employees of service providers who have access to information must comprehend their responsibilities on information security.

b. Roles and responsibilities of human resources such as Bank's employees, consultants, and employees of service providers who have access to information must be defined and documented in accordance with the policy of information security.

c. In the agreement and contract with Bank's employees, consultants, and employees of service providers, must be stated regulations regarding Information Technology security in accordance with Bank's information security policy.

d. Selain perjanjian antara Bank dengan perusahaan penyedia jasa, semua Karyawan perusahaan penyedia jasa tersebut yang ditugaskan di Bank harus menandatangani suatu perjanjian menjaga kerahasiaan informasi (*non-disclosure agreement*).

e. Pelatihan dan/atau sosialisasi tentang pengamanan informasi harus diberikan kepada Karyawan Bank, konsultan dan Karyawan pihak penyedia jasa. Pelatihan dan/atau sosialisasi ini diberikan sesuai dengan peran dan tanggung jawab Karyawan serta pihak penyedia jasa.

f. Bank harus menetapkan sanksi atas pelanggaran terhadap kebijakan pengamanan informasi.

g. Bank harus menetapkan prosedur yang mengatur tentang keharusan untuk mengembalikan aset dan pengubahan/penutupan hak akses Karyawan Bank, konsultan, dan Karyawan pihak penyedia jasa yang disebabkan karena perubahan tugas atau selesainya masa kerja atau kontrak.

3. Prosedur Pengamanan Fisik dan Lingkungan

a. Fasilitas pemrosesan informasi yang penting (misalnya *mainframe, server*, *PC*, perangkat jaringan aktif) juga harus diberikan pengamanan secara fisik dan lingkungan yang memadai untuk mencegah akses yang tidak terotorisasi, kerusakan serta gangguan lain.

d. Other than the agreement between Banks and service provider companies, all employees of said companies emplaced in the Bank must sign a agreement to safeguard the confidentiality of information (non-disclosure agreement).

e. Training and/or socialization about information security is obligatory for Bank's employees, consultants, and employees of service providers. This training and/or socialization are given in accordance with the roles and responsibilities of the employees as well as the service providers.

f. Banks must determine penalties for violations on policies of information security.

g. Banks must determine procedures which regulate issues regarding the obligation to return/restore assets and regarding changing/disabling the right of access of Bank's employees, consultants, and employees of service providers which are caused by duty reassignment or end of work period or contract.

3. Physical and Environmental Security Procedure

a. Important information processing facilities (such as mainframe, server, PC, active network equipment) must be secured physically and environmentally to avoid unauthorized access, damages as well as other disturbances.

b. Pengamanan fisik dan lingkungan terhadap fasilitas pemrosesan informasi yang penting meliputi antara lain pembatas ruangan, pengendalian akses masuk (misalnya penggunaan *access control card*, PIN), kelengkapan alat pengamanan di dalam ruangan (misalnya alarm, pendeteksi dan pemadam api, pengukur suhu dan kelembaban udara, *close-circuit* TV) serta pemeliharaan kebersihan ruangan dan peralatan (misalnya dari debu, rokok, makanan/minuman, barang mudah terbakar).

b. Physical and environmental security on important information processing facilities includes, amongst others, partitions, entry access control (such as the use of access control card, PIN), sufficiency of indoor security equipment (such as alarms, fire detectors and extinguishers, thermometers and hygrometers, close-circuit TV) as well as sanitation (from dust, cigarettes, food/drinks, flammables).

c. Fasilitas pendukung seperti AC, sumber daya listrik, *fire alarm* harus dipastikan kapasitas dan ketersediaannya dalam mendukung operasional fasilitas pemrosesan informasi.

c. The capacity and availability of supporting facilities such as AC, power source, fire alarms must be ensured to support the operations of information processing facilities.

d. Aset milik pihak penyedia jasa (seperti *server*, *switching tools*) harus diidentifikasikan secara jelas dan diberikan perlindungan yang memadai seperti misalnya dengan menerapkan pengamanan yang cukup, *dual control* atau menempatkan secara terpisah dari aset milik Bank.

d. Assets of service providers (such as server, switching tools) must be identified clearly and adequately protected, for example by implementing sufficient security, dual control or separate emplacement from Bank's assets

e. Melakukan pemeliharaan dan pemeriksaan secara berkala terhadap fasilitas pemrosesan informasi dan fasilitas pendukung sesuai dengan prosedur yang telah ditetapkan.

e. Periodic maintenance and assessment of information processing facilities and supporting facilities in accordance with predetermined procedures.

4. Prosedur Pengamanan *Logic*

4. Logical Access Control Procedure (Logical Security)

1. Bank memiliki prosedur formal tentang pengadministrasian *user* yang meliputi pendaftaran, perubahan dan penghapusan *user*, baik untuk *user* internal Bank maupun *user* eksternal Bank (misalnya vendor atau pihak penyedia jasa).

1. Banks have formal user administration procedures approved by the management) which include registration, change and removal, of internal or external user (such as vendor or service provider).

2. Bank harus menetapkan prosedur pengendalian melalui pemberian *password* awal (*initial password*) kepada *user* dengan memperhatikan antara lain hal-hal sebagai berikut:

2. Banks must determine internal control procedures by providing initial password to users with consideration to the following:

a. *Password* awal harus diganti saat *login* pertama kali.

b. *Password* awal diberikan secara aman, misalnya melalui amplop tertutup atau kertas berlapis dua.

c. *Password* awal bersifat khusus *(unique*) untuk setiap *user* dan tidak mudah ditebak.

d. Pemilik *User ID* terutama dari Karyawan Bank dan Karyawan pihak penyedia jasa harus menandatangani pernyataan tanggung jawab atau perjanjian penggunaan *User ID* dan *password* saat menerima *User ID* dan *password*.

e. *Password* standar (*default password*) yang dimiliki oleh sistem operasi, sistem aplikasi, *database management system*, dan perangkat jaringan harus diganti oleh *Bank* sebelum diimplementasikan dan sedapat mungkin mengganti *User* ID standar dari sistem (*default User ID*).

3. Bank harus mewajibkan *user* untuk:

3.1 Menjaga kerahasiaan *password*.

3.2 Menghindari penulisan *password* di kertas dan tempat lain tanpa pengamanan yang memadai.

3.3 Memilih *password* yang berkualitas yaitu:

a. Panjang password yang memadai sehingga tidak mudah ditebak.

b. Mudah diingat dan terdiri dari sekurang-kurangnya kombinasi 2 tipe karakter (huruf, angka atau karakter khusus).

c. Tidak didasarkan atas data pribadi user

a. Initial password must be changed at the time of the first login.

b. Initial password is given in a secure manner, such as through a sealed envelope or double-sided paper.

c. Initial password is unique to every user and unpredictable.

d. Owner of User ID especially from Bank's employees and employees of service providers must sign statement of responsibility or agreement of the use of User ID and password when receiving the User ID and password.

e. Default password of operation system, application system, database management system, and network equipment must be changed before being implemented and also change the default User ID.

3. Banks must require users to

3.1 Keeps password confidential.

3.2 Avoid writing passwords on paper and other places without adequate security.

3.3 Choosing a quality password, namely:

a. Have minimum sufficient length of password and not easily guessed.

b. Easy to remember and consist of at least a combination of 2 character types (letters, numbers or special characters).

c. Not based on user's personal information such

seperti nama, nomor telepon atau tanggal lahir.

d. Tidak menggunakan kata yang umum dan mudah ditebak oleh perangkat lunak misalnya kata 'pass', *'password'*, 'adm', atau kata umum di kamus.

3.4 Mengubah *password* secara berkala.

3.5 Menghindari penggunaan *password* yang sama secara berulang.

4. Bank harus menonaktifkan hak akses bila *user* id tidak digunakan pada waktu tertentu, menetapkan jumlah maksimal kegagalan *password* (*failed login attempt*) dan menonaktifkan *password* setelah mencapai jumlah maksimal kegagalan *password.*

5. Bank harus melakukan pemeriksaan/review berkala terhadap hak akses *user* untuk memastikan bahwa hak akses yang diberikan sesuai dengan wewenang yang diberikan.

6. Sistem operasi, sistem aplikasi, *database, utility* dan perangkat lainnya yang dimiliki oleh Bank sedapat mungkin membantu pelaksanaan pengamanan *password*, sebagai contoh:

1) Memaksa user untuk mengubah *password* nya setelah jangka waktu tertentu dan menolak bila *user* memasukkan *password* yang sama dengan yang digunakan sebelumnya saat mengganti *password.*

2) Menyimpan *password* secara aman.

3) Memutuskan hubungan atau akses *user* jika tidak terdapat respon selama jangka waktu tertentu *(session time-out).*

as names, phone numbers or date of birth.

d. Not use common words or words easy to guess by software (to avoid brute force attack), such as the word 'pass', 'password', 'adm', or words common in dictionaries.

3.4 Change the password periodically.

3.5 Avoid using the same password repeatedly.

4. Banks must deactivate the right of access if inactive for a certain period of time, determine the maximum amount of failed login attempt and deactivate a password after reaching the maximum failed attempt.

5. Banks must periodically review user access right to ensure it is in accordance with the given authorization.

6. Bank's operation systems, application systems, database, utilities and other equipments should help ensure the securing of password, for example:

1) Enforce users to change their password after a certain period of time and avoid historical password.

2) Store password securely.

3) Cut off the connection or user's access when there are no responses after a certain period of time (session time-out).

4) Menonaktifkan atau menghapus hak akses user jika *user* tidak melakukan *Log On* melebihi jangka waktu tertentu *(expiration interval*), misalnya karena cuti, pindah Divisi.

4) Deactivate or delete a user's access right if inactive Log On for a certain period of time (expiration interval), i.e. annual leave, relocation.

7. Bank harus memperhitungkan risiko dan menerapkan pengendalian pengamanan yang memadai dalam penggunaan media penyimpan data seperti *notebook, handphone, flash disk, external hard disk.*

7. Banks must estimate the risks and implement adequate control in the use of data storage media such as notebook, handphone, flash disk, and external hard disk.

8. Bank harus memperhitungkan risiko dan menerapkan pengendalian pengamanan yang memadai terhadap titik akses (*access point*) ke dalam jaringan komputer dan/atau sarana pemrosesan informasi yang dapat dimanfaatkan oleh pihak yang tidak berwenang.

8. Banks must estimate the risks and implement adequate control on network access points and/or information processing facility that can be used by unauthorized parties.

9. Bank yang menggunakan *file sharing* harus menetapkan pembatasan akses sekurang-kurangnya melalui penggunaan *password* dan pengaturan pihak yang berwenang melakukan akses.

9. Limit access for file sharing, at least enforce the use of password and user access management.

10. Bank perlu memperhatikan proses *security hardening* terhadap perangkat keras dan perangkat lunak, seperti: setting parameter, *patch.*

10. Bank considers the security hardening on hardware and software, such as: setting parameter, patch.

5. Prosedur Pengamanan Operasional Teknologi Informasi

1. Informasi dan perangkat lunak harus dibuatkan *backup* dan prosedur *recovery* yang teruji sesuai dengan tingkat kepentingannya.

2. Bank perlu mengantisipasi dan menerapkan pengendalian pengamanan yang memadai atas kelemahan sistem operasi, sistem aplikasi, *database* dan jaringan, termasuk ancaman dari pihak yang tidak berwenang seperti virus, *trojan horse*, *worms*, *spyware*, *Denial-Of-Service* (*DOS*), *war driving*, *spoofing* dan *logic bomb*.

5. Information Technology Operation Security Procedure

1. Information and software must have a backup and recovery procedure and tested according to its level of importance.

2. Bank needs to anticipate and implement adequate security control on operation system, application system, database and networks, including threats from unauthorized parties such as virus, Trojan horse, worms, spy ware, Denial-Of-Service (DOS), war driving, spoofing and logic bomb.

3. Bank memiliki kebijakan dan prosedur pengkinian anti virus dan patch dan memastikan pelaksanaannya (mengacu ke Kebijakan *Antivirus*).

4. Bank membuat prosedur yang mencakup identifikasi *patch* yang ada, melakukan pengujian, dan menginstalasinya jika memang dibutuhkan.

5. Bank memelihara catatan dari versi perangkat lunak yang digunakan dan memantau secara rutin informasi tentang pengkinian (*enhancement*) produk, masalah keamanan, *patch* atau *upgrade*, atau permasalahan lain yang sesuai dengan versi perangkat lunak yang digunakan.

6. menetapkan penggunaan enkripsi dengan menggunakan teknik kriptografi tertentu dalam mengamankan proses transmisi informasi yang sensitif, khususnya yang melalui jaringan di luar jaringan komunikasi Bank. Penggunaan teknik kriptografi tersebut antara lain ditujukan untuk menjaga dan memastikan kerahasiaan, integritas, keaslian, dan *non-repudiation*.

7. Bank harus menerapkan metode identifikasi dan otentikasi *(authentication)* sesuai tingkat pentingnya aplikasi (contoh: *log on id, password,* token atau *fingerprint)*.

8. Bank menyediakan dan melakukan kaji ulang atas jejak audit/*log* baik di tingkat jaringan, sistem maupun aplikasi serta menetapkan jenis log (misalnya *administrator log*, *user log, system log*), informasi yang harus dimasukkan ke dalam *log,* jangka waktu penyimpanan atau kapasitas *log* dengan memperhatikan ketentuan yang berlaku untuk keperluan penelusuran masalah.

6. Prosedur Penanganan Insiden dalam Pengamanan Informasi

a. Insiden yang terjadi harus dapat diidentifikasi, dilaporkan, ditindaklanjuti, didokumentasikan dan dievaluasi untuk memastikan dilakukannya penanganan yang

3. Bank have a formalize policies and procedures of anti-virus and patch updates, and ensure their Implementation (refer to Antivirus Policy).

4. Bank develops procedures which includes identification of existing patches, testing, and install it if necessary.

5. Bank maintains a record of current software version and routinely monitors the information regarding updates (enhancement) of products, security problems, patches or upgrades, or other roblems in accordance with the current software version.

6. Bank implements the use of encryption by using a particular cryptography technique in securing the process of sensitive information transmission, especially connection to external network, in accordance with the development of the latest technology. The uses of cryptography technique are, amongst others, aimed to safeguard and ensure confidentiality, integrity, authenticity, and non-repudiation.

7. Bank implement identification and authentication method in accordance with the level of importance of applications (example: log on id, password, token or fingerprint).

8. Bank provide and review audit trail/log in network, system or application level, as well as determine the type of the log (such as administrator log, user log, system log), information required in the log, storage duration or log capacity with consideration on valid regulation for problem trailing.

6. Information Security Incidents Response Procedure

a. Incidents must be identified, reported, acted upon, documented and evaluated to ensure proper handling and to avoid reoccurrence.

tepat dan untuk mencegah terulangnya insiden

b. Bank menetapkan prosedur penanganan insiden yang mengatur antara lain

1) Siapa yang harus melaporkan insiden.

2) Jenis insiden yang harus dilaporkan.

3) Alur pelaporan insiden.

4) Siapa yang bertanggung jawab untuk menindaklanjuti insiden.

5) Analisis atas insiden untuk mencegah terulangnya insiden.

6) Pendokumentasian bukti terkait insiden dan tindak lanjutnya.

c. Karyawan Bank dan karyawan pihak penyedia jasa diminta untuk melaporkan setiap kali menemukan indikasi atau potensi kelemahan pada sistem dan aplikasi sesuai kebijakan dan prosedur.

b. Banks determine procedures of incidents response which regulate

1) Who reports the incidents.

2) The type of incidents to be reported.

3) Flow of incident reporting.

4) Who is responsible to act upon incidents.

5) Analysis on incidents to avoid reoccurrence.

6) Documentation of incident-related evidence and follow up.

c. Bank's employees and service provider employees are required to report on every indication or potential of weakness on the system and application in accordance with the policy and procedure of security incident report.

D. Prosedur Pemilihan Penyedia Jasa

Di bawah ini adalah poin-poin yang dapat dipertimbangkan dalam pemilihan penyedia jasa:

1. Profil penyedia jasa berdasarkan profil perusahaan, referensi perusahaan dan laporan keuangan yang diaudit.
2. Kinerja penyedia jasa berdasarkan kemampuan perusahaan dalam menyediakan teknologi, jasa dan keahlian yang berkualitas yang sesuai dengan kebutuhan Bank.
3. Layanan purna jual penyedia jasa berdasarkan SLA (*Service Level Agreement*) atau ketersediaan jasa/layanan *support*.

D. Procedure of Outsourcing Selection

Following points are consideration in selecting outsourcing:

1. Outsourcing profile that base on company profile, company reference and audited financial report.
2. Outsourcing performance that base on company's ability in providing qualified technology, service and skill that conform to Bank requirements
3. Outsourcing support after sales that base on SLA (Service Level Agreement) or support/service availability.

E. Prosedur Manajemen Pengamanan Informasi

1. Informasi rahasia hanya diperkenakan untuk ditransfer melalui jaringan Bank atau disimpan ke media penyimpanan milik Bank.
2. Proses transfer data atau informasi ke media penyimpanan dapat

E. Procedure Information Security Management

1. Confidential information only allowed to transferred using Bank's network or saved to Bank's media storage.
2. Process of data or information transfer to media storage should using assigned computer.

dilakukan menggunakan komputer yang telah ditentukan.

3. Setiap karyawan yang berkewajiban untuk mematuhi/mengetahui tugas dan tanggung jawabnya sehubungan dengan sharing informasi baik secara internal maupun eksternal.

3. All employees responsible to follow/have knowledge of job and responsibility related to sharing information at internal or external.

4. Bank menetapkan prosedur pengamanan dalam pengiriman informasi ke pihak ketiga pengamanan informasi dalam menjamin keaslian dan kerahasiaan informasi.

4. Bank specifies security procedure to ensure information integrity and confidentiality in sending information to third party.

5. Bank menjamin kerahasiaan, keamanan data dan/atau infromasi pribadi Nasabah harus dilindungi dan diamankan dari akses yang tidak berhak sesuai dengan kebijakan internal dan peraturan yang berlaku.

5. The Bank guarantees the confidentiality, security of Customer's personal data and/or information must be protected and secured from unauthorized access in accordance with internal policies and applicable regulations.

6. Bank memastikan pengamanan data atau informasi dijalankan ketika menggunakan jasa pihak ketiga dalam memusnahkan peralatan atau material lainnya yang sudah tidak dipergunakan lagi.

6. Bank ensure data or information security when using third party in disposal unused equipment or other tools.

7. Hanya orang/pejabat yang diberi otorisasi saja yang dapat memberikan informasi mengenai segala sesuatunya yang berhubungan dengan perusahaan kepada media massa (misalnya surat kabar, televisi, radio, majalah, dan lain-lain).

7. Only authorized person that able to give company's information to mass media (such as newspaper, television, radio, magazine and others).

8. Seluruh karyawan diharapkan dapat menerapkan prinsip kebersihan meja kerja, dimana setiap meninggalkan meja kerja, maka semua dokumen dan data/informasi diamankan. Hal ini dimaksudkan untuk menghindari data/informasi dipindahkan, di-*copy,* dibuang, atau dicuri oleh orang yang tidak berhak.

8. All employees expected to ensure desk cleanliness and ensure all document and data/information is secured. The purpose is to prevent data/information is moved, copied or stolen by unauthorized person.

9. Karyawan Bank dilarang memberi komentar atau pendapat secara lisan atau tulisan melalui email, media massa dan sarana lainnya yang bersifat menghina/memfitnah orang/perusahaan lain, karena hal tersebut dapat dikenakan tindakan hukum.

9. Bank's employee is not allowed to give comment or opinion by verbal or by written using email, mass media or other tools that has purpose to offend/slander other person/company, because it can cause legal action.

10. Penggunaan email perusahaan untuk kepentingan pribadi harus

10. Using company email for personal use is strictly limited to prevent information security risk.

dibatasi untuk menghindari risiko pengamanan informasi.

11. Penggunaan telepon perusahaan untuk keperluan pribadi harus dibatasi dan diminimalkan, kecuali dalam kondisi darurat saja.

12. Seluruh data dan informasi yang tidak diperuntukkan untuk umum, baik informasi yang berhubungan dengan bisnis perusahaan maupun yang menyangkut karyawannya harus tetap dijaga kerahasiaannya. Seluruh karyawan dilarang membagi/memberikan informasi tersebut meskipun kepada anggota keluarganya sendiri.

13. Seluruh karyawan dilarang bergosip/membicarakan kondisi dan rahasia perusahaan ditempat-tempat umum untuk menghindari pihak-pihak yang tidak berkepentingan menggunakan informasi tersebut.

11. Using company telephone for personal use is limited and minimized, except in emergency condition.

12. All company data/information that is strictly limited for public should be secured. All employees is not allowed to give/share information even to own family.

13. All employees not allowed sharing rumors/talk about company's confidential information at public area to prevent unauthorized person using the information.

F. Prosedur Backup, Recovery, Archiving dan Restore

1. PIC Divisi TI bertanggung jawab untuk mengatur dokumentasi dari setiap sistem yang dipergunakannya. Hal ini dimaksudkan untuk memudahkan operasional dan pemeliharaan.

2. PIC Divisi TI memastikan bahwa dokumentasi mengenai teknik dan operasional sistem yang digunakan sudah disosialisasikan kepada seluruh karyawan pada Divisi/Seksi/Cabang yang bersangkutan untuk menghindari terhambatnya proses operasional dan menghindari ketergantungan terhadap satu orang.

3. PIC Divisi TI senantiasa memperbaharui dokumentasi sistem yang ada untuk memudahkan proses operasional. Dokumentasi yang sudah tidak berlaku (*out of date*) dapat menyebabkan kesulitan operasional.

4. Bank memastikan bahwa prosedur *recovery*, *backup* sistem dan data *backup* tersedia dan dapat digunakan sewaktu-waktu.

5. Karyawan dilarang melakukan proses *shutdown* komputer secara paksa kecuali dengan sepengetahuan dan

F. Procedure of Backup, Recovery, Archiving and Restore

1. IT Division PIC responsible to manage documentation of system used. The purpose is to ease operational and maintenance.

2. IT Division PIC ensures that technical documentation and the system operation are socialized to all related employee at Section/Division/Branch to prevent operational process delay and to prevent dependency to one person.

3. IT Division PIC continuously updated system documentation to ease operational process. Out of date document can cause operational difficulty.

4. Bank ensures that recovery procedure, system backup and backup data are available and can be used at any time.

5. Employees are not allowed to force shutdown computer except with acknowledge from System Administrator.

mendapat ijin dari *System Administrator.*

6. Informasi dan data yang disimpan dalam laptop atau PC harus di *backup* secara teratur. Proses *backup* merupakan tanggung jawab dari setiap pemakai.

7. Bank bertanggung jawab memastikan bahwa frekuensi *backup* seperti *backup* operasional dan prosedur pemulihan sudah sesuai dengan kepentingan bisnis perusahaan dan peraturan yang berlaku.

8. Prosedur pemulihan harus didokumentasikan secara jelas dan diujicoba secara teratur termasuk pengamanan informasi.

9. Bank memastikan bahwa keaslian data (*integrity*) selama proses pemulihan dan proses *restore* khususnya terhadap file-file yang bisa ditimpa (*replaced*) oleh file sebelumnya.

10. Media penyimpanan dan format data yang akan digunakan untuk proses *archiving* harus disesuaikan dengan lama masa penyimpanan dalam media tersebut.

6. Information and data saved in the laptop or PC requires backup process on regular basis. The backup process is responsibility of all users.

7. Bank responsible to ensure that backup frequency such as operational backup and recovery procedure is conform to company business and regulation.

8. Recovery procedure is documented and tested on regular basis including its information security.

9. Bank ensures data integrity during recovery and restore process, especially for files that can be replaced by previous file.

10. Storage media and data format used for data archive should adjust to retention period of the media.

G. Prosedur Lainnya

Selain ruang lingkup diatas, pengamanan informasi perlu diterapkan dalam aspek lain seperti pengembangan dan pengadaan sistem, jaringan komunikasi data, BCP dan DRP dan kegiatan penggunaan pihak penyedia jasa dalam penyelenggaraan TI yang masing-masing mengacu ke Kebijakan terkait.

G. Other Procedure

Other than the scope mentioned above, information security must be implemented in other aspects such as system development and establishment, data communication network, BCP and DRP and the activity of using IT service providers that refers to each related Policy.

H. Proses Manajemen Risiko

1. Penilaian Risiko

Bank mengelola seluruh sumber daya TI sebagai “aset” Bank. Sumber daya TI meliputi aplikasi, informasi, insfrastruktur dan sumber daya manusia. Bank harus melakukan evaluasi atas segala hal yang mengancam sumber daya TI melalui proses identifikasi, pengukuran dan pemantauan risiko potensial atau probabilitas kejadian maupun besarnya dampak.

H. Process of Risk Management

1. Risk Assessment

Bank manages every IT resource as an asset of the Bank. IT resources include, amongst others, applications, information, infrastructure and human resources. Therefore, Banks must perform evaluation on all that threaten IT resources through the process of identification, measurement and monitoring of potential risks in their tendency or probability of

Terdapat berbagai pendekatan yang dapat dilakukan Bank dalam proses identifikasi seperti pendekatan proses, aset, produk dan kejadian. Pada pendekatan berdasarkan aset, indentifikasi risiko pengamanan informasi dilakukan dengan melakukan klasifikasi terhadap "aset" terkait TI berdasarkan risiko.

Dalam menentukan aset yang kritikal maupun mengukur risiko, setiap satuan kerja harus dapat menentukan kemungkinan adanya ancaman (*threats*), serangan (*attacks*) dan kerawanan (*vulnerability*) dari setiap sumber daya TI yang digunakan masing-masing satuan kerja serta kemungkinan dampaknya pada integritas *(integrity),* kerahasiaan *(confidentiality)* dan ketersediaan *(availability)* dari data/informasi yang dimiliki. Proses ini harus dilakukan Bank karena identifikasi dan pengukuran risiko dapat menunjukkan potensial kegagalan atau kelemahan proses pengamanan informasi yang dapat berpengaruh pada kesuksesan bisnis Bank sehingga Bank dapat melakukan penanganan yang tepat terhadap setiap risiko potensial.

occurrence or the magnitude of the effect.

There are several approaches of identification such as approach by process, assets, products, and occurrences. In the approach based on assets, the identification of security risks are conducted through a classification on "assets" related to information technology based on risks.

In determining critical assets or measuring risks, each and every work unit must be able to determine the probability of threats, attacks and vulnerability from every IT resource used by each work unit as well as possible effects on integrity, confidentiality and availability of existing data/information. This process must be carried out because identification and measurement of risks can show the potential of failure or weakness of information security process which can influence the success of Bank's business so Banks are able to act proper response on every potential risk.

2. Pengendalian dan Mitigasi Risiko

Bank menetapkan bentuk penanganan risiko yang akan diterapkan untuk menimalisasi risiko yang dihadapi Bank. Dari bentuk-bentuk penanganan risiko (*accept, control/mitigate, avoid*, transfer), pengendalian dan atau mitigasi risiko memegang peranan penting karena tanpa sistem informasi yang handal dan aktivitas pengendalian TI yang efektif, Bank tidak mampu menghasilkan laporan keuangan yang akurat, terkini, utuh dan lengkap.

Bentuk pengendalian antara lain:

1. Kebijakan, ketentuan dan prosedur yang ada di Bank
2. Sistem pengendalian risiko yang dilakukan dengan menggunakan teknologi sehingga secara otomatis dapat memitigasi risiko yang ada yang digunakan sistem

2. Risk Management and Mitigation

Banks determine type of risk handling to be implemented. From type of risks response (accept, control/mitigate, avoid, transfer), risks control and/or mitigation holds an important role because without reliable information system and effective IT control activities, Banks will not be able to present accurate, latest, total and complete reports.

Type of controls are:

1. Policies, regulations and procedures in a Bank.
2. Risks control system using technologies so to automatically mitigate existing risks such as audit log, on line approval, parameter value in the system used.

seperti audit log atau parameter *value*.

3. Training dan *security awareness program*.

Bentuk pengendalian beragam dan tidak terbatas pada pengendalian umum *(general controls)* seperti pengendalian yang harus ada di operasional Data Center maupun yang berupa pengendalian aplikasi (*application controls*) seperti rekonsiliasi dalam *balancing control activities*. Dengan demikian atas seluruh aset Bank baik pada level Bank, satuan kerja maupun masing-masing petugas/pengguna TI dapat terhindar dari setiap risiko potensial.

3. Training and security awareness program.

Type of controls are vary and not limited to general controls such as controls that must be present in Data Center operations, or one in the form of application controls such as reconciliation in balancing control activities. And so every Bank's asset in the level of Bank, work unit or individual official/user can avoid potential risks.

I. Pengendalian *Intern* dan Audit

Divisi Audit (SKAI) harus melaksanakan program audit untuk memastikan bahwa pengendalian pengamanan informasi telah diterapkan, memadai dan berjalan secara efektif sesuai dengan kebijakan dan prosedur pengamanan informasi yang berlaku.

Divisi Audit (SKAI) wajib melaksanakan audit intern terhadap seluruh aspek dalam penyelenggaraan dan penggunaan Teknologi Informasi sesuai kebutuhan, prioritas, dan hasil analisis risiko Teknologi Informasi paling sedikit 1(satu) kali dalam 1(satu) tahun.

Evaluasi dan penyempurnaan terhadap kebijakan, prosedur dan program pengamanan informasi harus selalu dilakukan antara lain dengan melaksanakan pemantauan terhadap :

1. Perkembangan teknik atau metode baru yang mengancam sistem pengamanan informasi Bank

2. Laporan kinerja pengamanan informasi dalam rangka mengidentifikasi trend ancaman atau kelemahan kontrol pengamanan. Secara lebih spesifik kegiatan ini meliputi kaji ulang terhadap log aktivitas, investigasi anomali operasional dan evaluasi level akses terhadap sistem dan aplikasi TI.

3. Efektivitas penerapan kebijakan, prosedur dan pengendalian pengamanan informasi.

I. Internal Control and Audit

The Audit Division (SKAI) must carry out audit programs to ensure that information security control has been implemented, is adequate and running effectively in accordance with valid policies and procedures of information security.

The Audit Division (SKAI) is obliged to carry out internal audits of all aspects in the implementation and use of Information Technology according to the needs, priorities, and results of the Information Technology's most risk analysis at least 1 (one) year in 1 (one) year

Evaluation and completion on policies, procedures and programs of information security must always be conducted, amongst others by carrying out monitoring on:

1. Development of new techniques or methods that threaten Bank's information security system.

2. Reports of information security performance to identify trend of threats or weaknesses to security control. More specifically this activity includes review on activities log, operation anomaly investigation and routinely evaluate access levels on IT systems and applications.

3. The effectiveness of the implementation of information security policies, procedures and controls.

IV. PENUTUP

Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem Dalam Pengguna Teknologi Informasi Edisi 7 ini diterbitkan dalam 2 (dua) bahasa yaitu Bahasa Indonesia dan Bahasa Inggris dan bilamana terjadi perbedaan penafsiran antara keduanya maka yang menjadi acuan adalah Bahasa Indonesia.

Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem Dalam Penggunaan Teknologi Informasi Edisi 7 ini mulai berlaku sejak memperoleh persetujuan Presiden Direktur pada tanggal 19 Oktober 2022 dan Dewan Komisaris pada tanggal 2 November 2022 serta mencabut Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem dalam Penggunaan Teknologi Informasi ini Edisi 6, April 2021.

Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem ini akan dikaji ulang secara berkala, paling lambat setiap 2 (dua) tahun atau jika diperlukan sebagai upaya penyempurnaan sesuai dengan perkembangan usaha dan kebutuhan Bank atau perubahan peraturan yang mendasarinya.

IV. CLOSING

Information Security Policy and System Risk Management for Information Technology Users 7th Edition is published in 2 (two) languages, namely Indonesian and English and if there is a difference of interpretation between the two, the reference is Indonesian..

This Policy on Information Security and System Risk Management in the Use of Information Technology 7th Edition comes into effect after obtaining the approval of the President Director on the date of 19th October 2022 and the Board of Commissioners on the date of 2nd November 2022 and revoking the Policy on Information Security and System Risk Management in the Use of Information Technology 6th Edition, April 2021.

Information security and risk management system policy will be reviewed once a year on regular basis, at the latest 2 (two) years as an improvement effort following the business development and the need of Bank or following the changes of base regulation.