Bank Resona Perdania

KEBIJAKAN *INTERNET BANKING*
INTERNET BANKING POLICY

Edisi ke-10, Februari 2024

10th Edition, February 2024

BOD Approval No. 066/ITD/IT-PLN/IV/2024

BOC Approval No. 058/BOC/IV/2024-ITD/IT-PLN

DAFTAR ISI

Table of Content

I. PENDAHULUAN

A. Latar Belakang

Seiring dengan perkembangan layanan berbasis digital dengan dukungan pemanfaatan TI, diperlukan ruang bagi Bank untuk terus mengembangkan inovasi layanan digital demi memberikan layanan yang komprehensif dan lebih berorientasi kepada kebutuhan Nasabah.

Bahwa pengembangan layanan digital bagi bank perlu memerhatikan aspek manajemen risiko, keamanan data Nasabah, serta pelindungan konsumen sehingga perlu memerhatikan aspek manajemen risiko, keamanan data Nasabah, serta pelindungan konsumen.

Internet Banking adalah salah satu produk layanan digital yang disediakan oleh Bank dengan menggunakan pihak penyedia jasa TI. *Internet Banking* menyediakan layanan yang bersifat transaksional, baik transaksi finansial seperti *transfer*, deposito, dan pembayaran pajak maupun nonfinansial seperti *inquiry* saldo.

B. Acuan

1. Undang-Undang Republik Indonesia No. 7 tahun 1992 sebagaimana telah diubah dengan Undang-Undang Republik Indonesia No. 10 tahun 1998 tentang Perbankan;
2. Undang-Undang Republik Indonesia No. 11 Tahun 2008 sebagaimana telah diubah dengan UU No. 19 Tahun 2016, kedua dengan UU RI No.1 Tahun 2024 tentang Informasi dan Transaksi Elektronik;
3. Peraturan Pemerintah No.71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
4. Peraturan Menteri Komunikasi dan Informatika RI No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik;
5. Peraturan Menteri Komunikasi dan Informatika RI No.5 Tahun 2020 sebagaimana telah diubah dengan Peraturan Menteri Komunikasi dan Informatika RI

I. INTRODUCTION

A. Background

Along with the development of digital-based services supported by the use of IT, the Bank's needs to continue to develop digital service innovations to provide services that are comprehensive and more oriented to customer needs.

The development of digital services for banking needs to pay attention to aspects of risk management, customer data security, and consumer protection, so it is necessary to pay attention to aspects of risk management, customer data security, and consumer protection.

Internet banking is one of the digital services provided by the bank using IT service providers. Internet banking provides transactional services, both financial transactions such as transfers, deposits, and tax payments as well as non-financial transactions such as checking balances.

B. Reference

1. Law of the Republic of Indonesia Number 7 of 1992 as amended by Law of the Republic of Indonesia Number 10 of 1998 concerning Banking;
2. Law of the Republic of Indonesia No. 11 of 2008 as amended by Law no. 19 of 2016, secondly by Law No.1 Tahun 2024 concerning Information and Electronic Transactions;
3. Government Regulation No.71 of 2019 on Electronic System Maintenance and Transactions;
4. 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
5. Regulation of the Minister of Communication and Informatics of the Republic of Indonesia Number 5 of 2020 as amended by Regulation of the Minister of Communication

No.10 Tahun 2021 tentang Penyelenggara Sistem Elektronik Lingkup Privat;

6. POJK No. 18/POJK.03/2016 tentang Penerapan Manajemen Risiko Bagi Bank Umum.

   Sejak 30 Oktober 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 dicabut dan tidak berlaku oleh POJK No. 13/POJK.03/2021 tentang Penyelenggaraan Produk Bank Umum.

   POJK ini dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam POJK No.17 Tahun 2023 tentang Penerapan Tata Kelola Bagi Bank Umum.

7. SEOJK No. 34/POJK.03/2016 tanggal 1 September 2016 tentang penerapan Manajemen Risiko Bagi Bank Umum;

8. POJK No.11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum;

   POJK ini dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam POJK No.17 Tahun 2023 tentang Penerapan Tata Kelola Bagi Bank Umum.

9. SEOJK No.21/SEOJK.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.

10. POJK No.22 Tahun 2023 tentang Perlindungan Konsumen dan Masyarakat Di Sektor Jasa Keuangan ;

    Pada saat Peraturan Otoritas Jasa Keuangan ini mulai berlaku :

    a. Ketentuan pelaksana POJK No.6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan yang mengatur Pelindungan Konsumen

and Informatics of the Republic of Indonesia Number 10 of 2021 concerning Private Electronic System Operators;

6. POJK No. 18/POJK.03/2016 about Implementation of Risk Management for Public Bank;

   Since October 30, 2021, Article 20, Article 21, Article 22 and Article 24 in POJK No. 18/POJK.03/2016 on the Implementation of Risk Management for Commercial Banks were declared revoked and invalid by POJK No. 13/POJK.03/2021 on the Implementation of Commercial Bank Products.

   This POJK still remain as long as it does not conflict with the provisions of POJK No.17 of 2023 concerning Implementation of Governance for Commercial Banks.

7. SEOJK No. 34 / POJK.03 / 2016 dated September 1, 2016 about the application of Risk Management for Commercial banks;

8. POJK No.11/POJK.03/2022 concerning Implementation of Information Technology for Commercial Banks;

   This POJK still remain as long as it does not conflict with the provisions of POJK No.17 of 2023 concerning Implementation of Governance for Commercial Banks.

9. SEOJK No.21/SEOJK.03/2017 dated 6 June 2017 concerning Implementation of Risk Management in the Use of Information Technology by Commercial Banks;

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

10. POJK No.22 of 2023 concerning Consumer and Community Protection in the Financial Services Sector;

    When this Financial Services Authority Regulation comes into force:

    a. Provisions for implementing POJK No.6/POJK.07/2022 concerning Protection of Consumers and the Public in the Financial Services Sector which regulates Protection of Consumers and

dan Masyarakat di Sektor Jasa Keuangan; dan

b. Surat Edaran Dewan Komisioner OJK Republik Indonesia No.5/SEOJK.05/2022 tentang Produk Asuransi yang Dikaitkan dengan Investasi,

dinyatakan tetap berlaku sepanjang tidak bertentangan dengan Peraturan Otoritas Jasa Keuangan ini.

11. SEOJK No.14/SEOJK.07/2014 tanggal 20 Agustus 2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen;

    Ketentuan-ketentuan pelaksana yang mengatur Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan, dinyatakan tetap berlaku sepanjang tidak bertentangan dengan POJK No.6/POJK.07/2022 ini.

12. POJK No.18/POJK.07/2018 tentang Layanan Pengaduan Konsumen di Sektor Jasa Keuangan;

    Pasal 3, Pasal 4, Pasal 5, Pasal 7, Pasal 10, Pasal 11, Pasal 12, Pasal 15, Pasal 16, Pasal 19, Pasal 21, Pasal 22, Pasal 26, Pasal 27, Pasal 28, Pasal 29, Pasal 31, Pasal 32, Pasal 33, Pasal 42, Pasal 43, Pasal 44, dan Pasal 45

    POJK No.18/POJK.07/2018 ini dicabut oleh POJK No. 22 Tahun 2023 tentang Pelindungan Konsumen Dan Masyarakat Di Sektor Jasa Keuangan (PKM SJK).

13. SEOJK No.17/SEOJK.07/2018 tanggal 6 Desember 2018 tentang Pedoman Pelaksanaan Layanan Pengaduan Konsumen di Sektor Jasa Keuangan;

14. POJK No.21 Tahun 2023 tentang Layanan Digital oleh Bank Umum;

15. SEOJK No.29/SEOJK.03/2022 tanggal 27 Desember 2022 tentang Ketahanan Dan Keamanan Siber Bagi Bank Umum.

16. SEOJK No.24/SEOJK.03/2023 tentang Penilaian Tingkat Maturitas Digital Bank Umum.

the Public in the Financial Services Sector; and

b. Circular Letter of the OJK Board of Commissioners of the Republic of Indonesia No.5/SEOJK.05/2022 concerning Investment-Related Insurance Products,

is declared to remain valid as long as it does not conflict with this Financial Services Authority Regulation.

11. SEOJK No.14/SEOJK.07/2014 dated 20 August 2014 concerning Confidentiality and Security of Consumer Personal Data and/or Information;

    Implementing provisions governing Consumer and Public Protection in the Financial Services Sector are declared to remain valid as long as they do not conflict with POJK No.6/POJK.07/2022.

12. POJK No.18/POJK.07/2018 concerning Consumer Complaint Services in the Financial Services Sector;

    Article 3, Article 4, Article 5, Article 7, Article 10, Article 11, Article 12, Article 15, Article 16, Article 19, Article 21, Article 22, Article 26, Article 27, Article 28, Article 29, Article 31 , Article 32, Article 33, Article 42, Article 43, Article 44, and Article 45

    POJK No.18/POJK.07/2018 is revoked with POJK No. 22 of 2023 concerning Consumer and Community Protection in the Financial Services Sector (PKM SJK).

13. SEOJK No.17/SEOJK.07/2018 dated 6 December 2018 concerning Guidelines for Implementing Consumer Complaint Services in the Financial Services Sector;

14. POJK No.21 of 2023 concerning Digital Services by Commercial Banks.

15. SEOJK No.29/SEOJK.03/2022 dated 27 December 2022 concerning Cyber Security and Resilience for Commercial Banks.

16. SEOJK No.24/SEOJK.03/2023 concerning Assessment of Digital Maturity Levels of Commercial Banks.

17. PADG No.20 Tahun 2023 tentang Tata Cara Pelaksanaan Perlindungan Konsumen Bank Indonesia.
18. Kebijakan Manajemen Risiko secara Umum (Individual);
19. Kebijakan Manajemen Risiko Teknologi Informasi;
20. Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem dalam Penggunaan Teknologi Informasi;
21. SOP Internet Banking – Perdania Direct
22. SOP Analisis Kejadian Risiko Operasional
23. Kebijakan Manajemen Proyek dan Pengembangan Sistem
24. Kebijakan Penggunaan Pihak Penyedia Jasa TI
25. Pedoman Pengadaan Barang dan Jasa Terkait TI
26. Pedoman Penilaian Risiko Keamanan Aplikasi
27. Kebijakan Pengawasan Keamanan Sistem dan Informasi
28. Pedoman Penanganan Insiden Keamanan Informasi
29. Kebijakan Perlindungan Konsumen dan Masyarakat
30. Kode Etik Pelindungan Nasabah
31. Kebijakan Tugas & Wewenang;
32. Kebijakan Job Description.

17. PADG No.20 of 2023 concerning Procedures for Implementing Bank Indonesia Consumer Protection
18. Individual General Risk Management Policy;
19. Risk Management of Information Technology;
20. Information Security and System Risk Management Policy in the use of Information Technology;
21. SOP Internet Banking – Perdania Direct
22. SOP Analysis of Operational Risk Events
23. Project Management and System Management Policy
24. The Use of IT Service Provider Policy
25. Procurement of Goods Related IT Guidelines
26. Application Security Risk Assessment Guidelines
27. System and Information Security Monitoring Policy
28. Handling Information Security Incidents Guidelines
29. Consumer and Community Protection Procedures
30. Customer Protection Code of Conduct
31. Duties & Authorities Policy;
32. Job Description Policy.

C. Tujuan

Kebijakan *Internet Banking* dibuat dan ditetapkan dengan tujuan :

1. Sebagai acuan dalam penerapan prosedur identifikasi, pengukuran, pemantauan dan pengendalian berbagai risiko yang melekat pada produk dan aktivitas *Internet Banking*
2. Memberikan pemahaman bagi seluruh pihak terkait produk dan aktivitas *Internet Banking*.

C. Purpose

The objectives of creating and enforcing the Internet Banking Policy are:

1. As a reference in carrying out procedure for identifying, measuring, monitoring, and controlling various risks inherent in Internet banking products and activitie
2. Provide understanding to all parties regarding Internet Banking products and activities.

3. Sebagai acuan dalam pemenuhan prinsip pengendalian pengamanan data Nasabah dan transaksi *Internet Banking*.

4. Sebagai acuan dalam penanganan keadaan tidak normal atau darurat ketika aplikasi Internet Banking tidak dapat digunakan karena gangguan atau bencana.

3. As a reference in fulfilling the principles of controlling customer data security and Internet banking transactions

4. As a reference in handling abnormal or emergency situations when the Internet Banking application cannot be used due to disruption or disaster.

II. TUGAS DAN TANGGUNG JAWAB

A. Dewan Komisaris

1. Mengevaluasi, mengarahkan, dan memantau kebijakan Bank terkait aktivitas *Internet Banking.*
2. Mengevaluasi pertanggungjawaban Direksi atas penerapan manajemen risiko terkait aktivitas *Internet Banking*.

B. Direksi

1. Direksi melakukan kaji ulang terhadap rencana pelaksanaan layanan *Internet Banking* yang berpotensi memiliki dampak yang signifikan terhadap strategi dan profil risiko Bank termasuk analisa cost dan benefit dari rencana layanan Internet Banking tersebut.
2. Direksi memastikan bahwa Bank pada saat memasuki aktivitas layanan Internet Banking telah memiliki manajemen risiko yang memadai. Selain itu Direksi harus memastikan bahwa pejabat atau pegawai yang terkait dengan aktivitas layanan Internet Banking memiliki kompetensi dalam aplikasi dan teknologi pendukung layanan Internet Banking.
3. Direksi memastikan bahwa proses Manajemen Risiko aktivitas layanan Internet Banking terintegrasi dalam Manajemen Risiko Bank secara keseluruhan serta melakukan pemantauan secara berkala terhadap risiko-risiko yang melekat pada layanan Internet Banking, dan melaporkan hasil pemantauan tersebut kepada Dewan Komisaris.

C. Fungsi Operasional dan Dukungan TI

1. Bertanggung jawab dalam penyelenggaraan *Internet Banking* dalam hal memberikan pelayanan dan memantau transaksi *Internet Banking* sebagaimana telah diatur dalam SOP *Internet Banking.*
2. Bertanggung jawab dalam penanganan masalah terkait aktivitas *Internet Banking* dengan berkoordinasi dengan Divisi terkait maupun penyedia jasa TI sebagaimana telah diatur dalam SOP *Internet Banking*.

II. JOB AND RESPONSIBILITY

A. Board of Commissioners

1. Evaluate, direct and monitor Bank policies regarding Internet Banking activities.
2. Evaluate the responsibility of the Board of Directors for implementing risk management related to Internet Banking activities

B. Board of Directors

1. The BoD reviews plans for implementing Internet Banking services that have the potential to have a significant impact on the Bank's strategy and risk profile, including analyzing the costs and benefits of Internet Banking service plans**.**
2. The BoD ensures that the Bank, when entering Internet Banking service activities, has adequate risk management. In addition, the Board of Directors must ensure that officials or employees related to Internet Banking service activities have competence in the applications and technology supporting Internet Banking services.
3. The BoD ensures that the Risk Management process for Internet Banking service activities is integrated into the Bank's overall Risk Management and carries out regular monitoring of the risks inherent in Internet Banking services, and reports the results of this monitoring to the BoC

C. IT Operations and Support Functions

1. Responsible for organizing Internet Banking in terms of providing services and monitoring Internet Banking transactions as regulated in the SOP Internet Banking.
2. Responsible for handling problems related to Internet Banking activities by coordinating with related divisions and IT service providers as regulated in the Internet Banking SOP.

3. Bertanggung jawab atas proses perbaikan pada sistem *Internet Banking* dan ikut serta dalam proses pengembangan sistem *Internet Banking.*

4. Berkoordinasi dengan Departemen *Complaint Handling and Customer Protection* dalam menangani pengaduan terkait layanan *Internet Banking*.

5. Bertanggung jawab atas ketersediaan dan kecukupan manual dan dokumentasi sistem terkait *Internet Banking*.

6. Berkoordinasi dengan Divisi terkait dalam mengedukasi Nasabah antara lain mengenai hak, kewajiban, manfaat dan risiko terkait dengan penggunanan layanan *Internet Banking*.

7. Melakukan pemantauan dan pemeliharaan terkait *hardware* dan *software* serta sistem pendukung lainnya terkait *Internet Banking.*

8. Memastikan proses rutin harian *(backup data* dan *end of day)* berjalan baik.

9. Berkoordinasi dengan pihak terkait dalam aktivitas rencana keberlangsungan usaha *Internet Banking* serta dalam pelaksanaannya saat terjadi kegagalan sistem yang dikarenakan gangguan.

D. Departemen Sistem TI

1. Memastikan *core banking system* berjalan Normal sehingga layanan *Internet Banking* dapat berjalan baik.

2. Berkoordinasi dengan pihak terkait dalam hal perbaikan sistem Internet Banking terkait dengan core banking system.

3. Berkoordinasi dengan pihak terkait dalam proyek pengembangan Internet Banking.

4. Berkoordinasi dengan pihak terkait dalam aktivitas rencana keberlangsungan usaha Internet Banking serta dalam pelaksanaannya saat terjadi kegagalan sistem yang dikarenakan gangguan.

E. Fungsi Proyek TI

1. Berkoordinasi dengan Divisi terkait dalam pengembangan *Internet Banking* agar dapat memenuhi kebutuhan dan ekspektasi Nasabah.

3. Responsible for the process of improving the Internet banking system and participating in the process of developing the Internet Banking system.

4. Coordinate with the Complaint Handling and Customer Protection Department in handling complaints related to Internet Banking services.

5. Responsible for the availability and adequacy of manuals and system documentation related to Internet Banking.

6. Coordinate with related divisions in educating customers, including rights, obligations, benefits, and risks related to the use of Internet Banking services.

7. Monitor and maintain hardware and software, as well as other supporting systems related to Internet Banking.

8. Ensure daily routine processes (data backup and end of day) run well.

9. Coordinate with related parties in planning activities for Internet banking business continuity and implementation in the event of system failure due to disruption.

D. IT System Department

1. Ensure that the core banking system is running normally so that Internet banking services can run well.

2. Coordinate with related parties in improving the Internet banking system related to the core banking system.

3. Coordinate Internet Banking development Projects.

4. Coordinate with related parties in planning activities for Internet banking business continuity and implementation in the event of system failure due to disruption gangguan.

E. IT Project Functions

1. Coordinate with the related Division in the development of Internet banking so that it can meet customer needs and expectations.

2. Bertanggung jawab dalam pelaksanaan proyek terkait Internet Banking sebagaimana telah diatur dalam Kebijakan Manajemen Proyek dan Pengembangan Sistem dan atau Kebijakan Penggunaan Pihak Penyedia Jasa TI.

2. Responsible for implementing projects related to Internet banking as regulated in the Project Management and System Development Policy and/or IT Service Provider Utilization Policy.

F. Departemen Perencanaan TI

1. Bertanggung jawab dalam pengadaan *Hardware* dan *Software* terkait *Internet Banking* sebagaimana telah diatur dalam Pedoman Pengadaan Barang dan Jasa terkait TI.

2. Bertanggung jawab terkait infrastruktur keamanan sistem dan jaringan terkait *Internet Banking.*

3. Berkoordinasi dengan Divisi terkait dalam aktivitas rencana keberlangsungan usaha *Internet Banking* serta dalam pelaksanaannya saat terjadi kegagalan sistem yang dikarenakan gangguan.

F. IT Planning Department

1. Responsible for the procurement of hardware and software related to Internet Banking as regulated in the Guidelines for Procurement of IT-related Goods and Services.

2. Responsible for the infrastructure and security of systems and networks related to Internet Banking.

3. Coordinate with related divisions in activities for Business Continuity Plan of Internet Banking Applications and implementation in the event of system failure due to disruption.

G. Departemen Keamanan Informasi dan Pengawas Risiko Sistem

1. Mengidentifikasi, melakukan analisis atas risiko terkait aktivitas sistem *Internet Banking* dengan mengacu kepada Kebijakan Manajemen Risiko Teknologi Informasi.

2. Bertanggung jawab menjaga Ketahanan dan Keamanan Siber dan melakukan Pengawasan Sistem sebagaimana telah diatur dalam Pedoman Penilaian Risiko Keamanan Aplikasi dan Kebijakan Pengawasan Keamanan Sistem dan Informasi.

3. Berkoordinasi dengan Divisi TI dalam Penangan Insiden Keamanan Informasi untuk fokus melindungi sistem informasi ataupun perangkat TI saat terjadi gangguan atau bencana, sebagaimana telah diatur dalam Pedoman Penanganan Insiden Keamanan Informasi

4. Berkoordinasi dengan Divisi TI dalam pelaporan Penilaian Tingkat Maturitas Digital Bank Umum.

G. Information Security and System Risk Controller Department

1. Identify and analyze risks related to Internet Banking system activities by referring to the Information Technology Risk Management Policy.

2. Responsible for maintaining cyber resilience and security and carrying out system supervision as regulated in the Application Security Risk Assessment Guidelines and System and Information Security Supervision Policy.

3. Coordinate with the IT Division in handling information security incidents to focus on protecting information systems or IT devices when a disruption or disaster occurs, as regulated in the Information Security Incident Handling Guidelines.

4. Coordinate with the IT Division in reporting the Commercial Bank Digital Maturity Level Assessment.

H. Divisi Internal Audit

1. Melakukan penilaian efektifitas pelaksanaan manajemen risiko aktivitas *Internet Banking*.

2. Memastikan pengendalian pengamanan telah mencukupi.

H. Internal Audit Division

1. Assess the effectiveness of implementing risk management in Internet banking activities.

2. Ensure the security controls are adequate.

III. MANAJEMEN RISIKO AKTIVITAS LAYANAN *INTERNET BANKING*

A. Pengukuran Risiko Layanan *Internet Banking*

Penggunaan Layanan Perbankan Digital berpotensi meningkatkan risiko antara lain risiko operasional, risiko compl, dan risiko reputasi. Pengukuran Risiko dilakukan terhadap potensi kerugian yang terjadi pada layanan *Internet Banking*. Untuk dapat memantau besar dan kecenderungan risiko dari layanan *Internet Banking* maka Bank harus membuat *database* yang berisi data historis kerugian *(loss event database)* sebagaimana telah diatur pada SOP Analisis Kejadian Risiko Operasional.

Risiko terkait penyelenggaraan layanan digital antara lain :

1. Risko Operasional yaitu risiko yang timbul atau berasal dari *fraud*, kesalahan dalam proses, gangguan sistem yang menyebabkan ketidakmampuan Bank untuk menyediakan layanan serta menimbulkan kerugian bagi Bank maupun Nasabah.

   Risiko operasional juga dapat mencakup risiko terkait transaksi yang merupakan risiko yang dapat timbul dari kurang memadainya pelaksanaan prinsip pengendalian pengamanan.

2. Risiko hukum mengingat transaksi melewati batas wilayah hukum yang berbeda. Risiko ini timbul karena terdapat perbedaan ketentuan peraturan perundang-perundangan di antara kedua wilayah hukum, seperti perlindungan konsumen, kerahasiaan Bank dan data pribadi Nasabah, persyaratan pelaporan, dan anti pencucian uang dan pencegahan pendanaan terorisme.

3. Risiko reputasi yaitu risiko yang timbul dari kemungkinan menurunnya atau hilangnya kepercayaan nasabah karena *service level delivery* kepada, kelambatan respon atas komplain Nasabah, ketidakamanan sistem, dan adanya gangguan pada sistem.

Risiko dalam penyelenggaraan *Internet Banking* meliputi:

III. INTERNET BANKING SERVICE RISK MANAGEMENT

A. Measurement of Internet Banking Service Risk

The use of digital banking services has the potential to increase risks, including operational risk, legal risk, and reputation risk. Risk measurement is carried out on potential losses that occur in Internet Banking services. To be able to monitor the magnitude and trend of risk from Internet Banking services, the bank must create a database containing historical loss data (loss event database) as regulated in the SOP Operational Risk Event Analysis.

Risks associated with providing digital services include :

1. Operational risk, namely risk arising or originating from fraud, process errors, or system disruptions that cause the bank's inability to provide services and cause losses for the bank and customers,

   Operational risks can also include transaction-related risks, namely risks that can arise as a result of inadequate implementation of security control principles.

2. Legal risk, considering that transactions cross different legal boundaries. This risk arises due to differences in legal and regulatory provisions between the two jurisdictions, such as consumer protection, confidentiality of bank and customer personal data, reporting requirements, anti-money laundering, and prevention of terrorist financing.

3. Reputation risk is the risk that arises from the possibility of reduced or lost customer trust due to the delivery of service levels, slow responses to customer complaints, system insecurity, and system disruption.

Risks in implementing Internet Banking include:

1. Nasabah memperoleh informasi yang salah atau tidak akurat melalui *Internet Banking;*

2. Pencurian data finansial dari Pangkalan Data *(Database)* Bank melalui *informational and communicative Internet Banking* yang tidak terisolasi;

3. Terdapat ancaman atau serangan misalnya *defacing, cybersquatting, denial of service*, pemutusan jaringan (network interception), *man-in-the middle-attack*, dan virus;

4. Pencurian identitas *(identity theft)* misalnya *phising, key logger, spoofing,* dan *cybersquatting;* dan

5. Terjadi transaksi yang dilakukan oleh pihak yang tidak berwenang *(unauthorized transaction)* atau terjadi *fraud.*

B. Pengendalian Risiko Layanan *Internet Banking*

Berikut pengendalian Risiko untuk Layanan *Internet Banking :*

1. Bank harus memperhatikan kenyamanan dan kemudahan Nasabah menggunakan fasilitas, termasuk efektivitas menu tampilan *Internet Banking* khususnya dalam melakukan pilihan pesan yang diinginkan Nasabah agar tidak terjadi kesalahan dan kerugian dalam transaksi.

2. Dalam rangka meningkatkan pengamanan, Bank dapat menetapkan persyaratan atau melakukan pembatasan transaksi melalui untuk menjamin keamanan dan keandalan transaksi, misalnya meminta Nasabah melakukan registrasi rekening pihak ketiga yang merupakan tujuan *transfer* dalam *Internet Banking* atau membatasi nominal jumlah transaksi melalui *Internet Banking.*

3. Bank harus memastikan terdapatnya pengamanan atas aspek transmisi data antara terminal *Electronic Fund Transfer (EFT)* dengan *host computer*, terhadap risiko kesalahan transmisi, gangguan jaringan, akses oleh pihak yang tidak bertanggung jawab, dan lain-lain. Pengamanan mencakup pengendalian terhadap peralatan yang digunakan, pemantauan terhadap akses perangkat lunak *Controller (Host-Front End),*

1. The customer obtains wrong or inaccurate information via Internet Banking;

2. Theft of financial data from the bank database via informational and communicative internet banking, which is not isolated;

3. There are threats or attacks, for example, defacing, cybersquatting, denial of service, network interception, man-in-the-middle, and viruses;

4. Identity theft, for example, phishing, key loggers, spoofing, and cybersquatting; And

5. There are transactions carried out by unauthorized parties (unauthorized transactions), or fraud occurs.

B. Internet Banking Service Risks Control

The following are risk controls for Internet Banking services :

1. Banks must pay attention to the comfort and convenience of customers in using facilities, including the effectiveness of the Internet Banking menu display, especially in selecting messages that customers want to avoid errors and losses in transactions.

2. To increase security, the bank may set requirements or place transaction restrictions to ensure the security and reliability of transactions, for example, by asking customers to register a third-party account for transfer purposes in Internet banking or limiting the nominal amount of transactions via Internet banking.

3. Banks must ensure the security of data transmission aspects between the Electronic Fund Transfer (EFT) terminal and the host computer against the risk of transmission errors, network disruption, access by irresponsible parties, etc. Security includes controlling the devices used, monitoring controller software access (host-front end), and monitoring the quality and accuracy of the performance of network devices and transmission

pemantauan kualitas dan akurasi kinerja perangkat jaringan serta saluran transmisi.

C. Pengendalian Pengamanan Data dan Transaksi Nasabah

Dalam rangka pengendalian risiko, Bank harus melakukan mitigasi atas yang mungkin terjadi dalam Layanan Perbankan Digital dengan memperhatikan pengendalian pengamanan data dan transaksi Nasabah.

Bank wajib menerapkan prinsip pengendalian pengamanan data dan transaksi Nasabah dari Layanan Digital pada setiap sistem elektronik yang digunakan oleh Bank mencakup paling sedikit prinsip :

1. Kerahasiaan *(confidentiality)*

Bank memastikan bahwa metode dan prosedur yang digunakan dapat melindungi kerahasiaan data Nasabah.

2. Integritas *(integrity)*

Bank memastikan bahwa metode dan prosedur yang digunakan mampu menjamin data yang digunakan akurat, andal, konsisten, dan terbukti kebenarannya sehingga terhindar dari kesalahan, kecurangan, manipulasi, penyalahgunaan, dan perusakan data.

3. Ketersediaan *(availability)*

Bank memastikan ketersediaan layanan dan Sistem Elektronik yang digunakan untuk menghasilkan data Nasabah secara berkesinambungan.

4. Keaslian *(authentication)*

Bank harus dapat menguji keaslian identitas nasabah untuk memastikan informasi yang disampaikan dan/atau transaksi keuangan dilakukan oleh nasabah yang berhak.

5. Tidak terbantahkan *(Non Repudiation)*

Bank harus menyusun, menetapkan, dan melaksanakan prosedur yang dapat memastikan bahwa transaksi yang telah dilakukan nasabah tidak dapat diingkari dan dapat dipertanggungjawabkan.

channels.

C. Security Control of Customer Data and Transactions

To control risks, banks must mitigate what might happen to digital banking services by paying attention to controlling the security of customer data and transactions.

Banks are required to apply the principles of controlling the security of customer data and transactions from digital services to every electronic system used by the bank, at least including the following principles:

1. Confidentiality

The bank ensures that the methods and procedures used can protect the confidentiality of customer data

2. Integrity

The bank ensures that the methods and procedures used are able to guarantee that the data used is accurate, reliable, consistent, and proven to be correct so as to avoid errors, fraud, manipulation, misuse, and destruction of data.

3. Availability

The bank ensures the availability of services and electronic systems used to generate customer data on an ongoing basis.

4. Authentication

Banks must be able to test the authenticity of customer identities to ensure that the information submitted and/or financial transactions are carried out by authorized customers.

5. Non Repudiation

Banks must prepare, establish and implement procedures that can guarantee that transactions carried out by customers cannot be denied and can be accounted for.

6. Pengendalian otorisasi dalam sistem, pangkalan data *(database)* dan aplikasi *(authorization of control)*

Bank memastikan antara lain:

a. Adanya pengendalian terhadap hak akses dan otorisasi yang tepat terhadap sistem, Pangkalan Data *(Database)* dan aplikasi yang digunakan dalam penyelenggaraan TI; dan.

b. Seluruh informasi dan data penyelenggaraan TI yang bersifat rahasia hanya dapat diakses oleh pihak yang telah memiliki otorisasi serta harus dipelihara secara aman dan dilindungi dari kemungkinan diketahui atau dimodifikasi oleh pihak yang tidak berwenang.

7. Pemisahan tugas dan tanggung jawab *(segregation of duties).*

Bank memastikan terdapat pemisahan tugas dan tanggung jawab terkait sistem, Pangkalan Data *(Database)* dan aplikasi yang digunakan dalam penyelenggaraan TI untuk terlaksananya fungsi check and balance, misalnya terdapat pemisahan tugas antara pihak yang menginisiasi atau meng-input data dengan pihak yang bertanggung jawab untuk memverifikasi dan/atau mengotorisasi kebenaran data tersebut

8. Pemeliharaan jejak audit *(maintenance of audit trails)*

Bank memastikan ketersediaan dan pemeliharaan log transaksi sesuai dengan kebijakan retensi data dan ketentuan peraturan perundang-undangan, agar terdapat jejak audit yang jelas untuk membantu pembuktian, penyelesaian perselisihan, dan pendeteksian usaha penyusupan pada Sistem Elektronik. Bank harus menganalisis dan mengevaluasi fungsi jejak audit secara berkala

9. Retensi data, termasuk penghapusan dan pemusnahan

Bank harus memelihara log transaksi berdasarkan kebijakan retensi data Bank sesuai ketentuan peraturan perundang-

6. Authorization of control on systems, databases and applications (authorization of control)

Bank ensure the following :

a. There are controls over appropriate access rights and authorization for systems, databases and applications used in IT operations; and.

b. All confidential IT information and data can only be accessed by authorized parties and must be kept safe and protected from the possibility of being discovered or changed by unauthorized parties

7. Segregation of Duties

The Bank ensures that there is a separation of duties and responsibilities related to systems, databases and applications used in IT operations to carry out check and balance functions, for example there is a separation of duties between those who initiate or input data and those who input data. The party responsible for verifying it. And/or validate the correctness of the data.

8. Maintenance of Audit Trails

The bank ensures the availability and maintenance of transaction logs in accordance with data storage policies and statutory provisions so that there is a clear audit trail to assist in the verification, dispute resolution, and detection of attempts to infiltrate the electronic system. Banks are required to analyze and evaluate the audit trail function periodically.

9. Data Retention includes deleting and destroying

Banks are required to maintain transaction records based on the bank’s data storage policy in accordance with statutory provisions.

undangan.

Bank selain harus memperhatikan pengamanan layanan terhadap Nasabah juga memperhatikan pengamanan serta hak dan kewajiban pihak lain yang terkait dan/atau yang bekerja sama dengan Bank dalam menyelenggarakan Layanan Perbankan Elektronik, khususnya terkait pengelolaan, penggunaan, dan penyimpanan data nasabah Layanan Perbankan Elektronik.

Banks must not only pay attention to securing services for customers but also to security and the rights and obligations of other parties related to and/or collaborating with the bank in providing electronic banking services, especially regarding management, use, and storage. Electronic Banking Service customer data.

D. Pelindungan Nasabah dan Pelindungan Data Pribadi

Bank yang menyelenggarakan layanan digital harus menerapkan prinsip perlindungan konsumen dan Data Pribadi. Prosedur Pelindungan Nasabah dan Pelindungan Data Pribadi dapat mengacu pada Kebijakan Perlindungan Konsumen dan Masyarakat dan Kode Etik Pelindungan Nasabah.

D. Customer Protection and Personal Data Protection

Banks providing digital services are required to implement the principles of consumer and personal data protection as regulated in the Consumer and Community Protection Policy and the Customer Protection Code of Ethics.

IV. AKTIVITAS OPERASIONAL *INTERNET BANKING*

A. Layanan Internet Banking

Unit/fungsi yang bertugas menangani penyelenggaraan Layanan Digital memiliki tugas paling sedikit :

1. Menyusun kebijakan, standar, dan prosedur penyelenggaraan Layanan Digital;
2. Memastikan kesesuaian antara penyelenggaraan Layanan Digital dengan rencana strategis kegiatan usaha Bank;
3. Memantau pelaksanaan kerja sama dengan mitra Bank dalam penyelenggaraan Layanan Digital;
4. Memantau data transaksi keuangan Layanan Digital;
5. Memastikan efektivitas langkah yang digunakan dalam menyelenggarakan Layanan Digital;
6. Memantau kendala dan permasalahan yang muncul dari penyelenggaraan Layanan Digital; dan
7. Memastikan kecukupan dan alokasi sumber daya terkait Layanan Digital yang dimiliki Bank.

Ref. Pasal 18 POJK No. 21 Tahun 2023 tentang Layanan Digital Oleh Bank Umum;

Saat ini penyelenggaraan layanan *Internet Banking* dilaksanakan oleh Divisi TI yaitu Fungsi Operasional dan Dukungan TI/IB *Helpdesk.*

Dalam hal penyelenggaraan layanan *Internet Banking* dilakukan oleh pihak lain *(outsourcing)*, Bank menetapkan dan menerapkan prosedur pengawasan dan *due diligence* yang menyeluruh dan berkelanjutan untuk mengelola hubungan Bank dengan pihak lain.

Nasabah yang dapat mengakses *Internet Banking* adalah Nasabah yang terdaftar pada Internet Banking sebagaimana telah diatur dalam SOP *Internet Banking.*

Untuk dapat mengakses aplikasi *Internet*

IV. INTERNET BANKING OPERATIONAL ACTIVITIES

A. Internet Banking Services

Unit/function that handles the implementation of Digital Services has at least the following tasks:

1. Develop policies, standards and procedures for providing Digital Services;
2. Ensure conformity between the implementation of Digital Services and the strategic plan for the Bank's business activities;
3. Monitor the implementation of collaboration with Bank partners in providing Digital Services;
4. Monitoring Digital Services financial transaction data;
5. Ensure the effectiveness of the steps used in providing Digital Services;
6. Monitor obstacles and problems that arise in the implementation of Digital Services; and
7. Ensure the adequacy and allocation of resources related to Bank Digital Services.

Ref. Article 18 POJK No. 21 of 2023 concerning Digital Services by Commercial Banks;

Currently, the implementation of Internet banking services is carried out by the Information Technology Division that is IT Operations and Support Functions/IB Helpdesk

When the implementation of Internet banking services is carried out by third party (outsourcing), the bank establishes and implements comprehensive and continuous monitoring and due diligence procedures to manage the bank’s relationship with other parties.

Customers who can access Internet Banking are those who are registered with Internet Banking as regulated in the SOP Internet Banking.

Banking, Nasabah harus menggunakan user id dan *password* yang telah didaftarkan.

To be able to access the Internet Banking application, the customer must use the registered user ID and password.

B. Operasional Sistem

Dalam penyelenggaraan *Internet Banking* semua sistem dan aplikasi yang terkait harus dipastikan berjalan dengan baik sesuai dengan prosedur yang berlaku.

B. System Operations

In the implementation of Internet Banking, all related systems and applications must be ensured to run properly in accordance with applicable procedures.

C. Aktivitas Transaksional Internet Banking

Nasabah pengguna dapat menggunakan layanan *Internet Banking* untuk mendapatkan informasi dan/atau melakukan transaksi perbankan yang telah disediakan oleh Bank.

Dalam layanan *Internet Banking*, Nasabah pengguna dapat melakukan :

1. Transaksi Finansial
2. Transaksi Non Finansial

Dalam Transaksi Finansial Bank wajib memastikan kesesuaian atas data dan/atau informasi yang dimanfaatkan dalam *Internet Banking*. Kesesuaian atas data dan/atau informasi yang dimanfaatkan dilakukan antara lain melalui perekaman langsung, verifikasi terhadap sumber data, dan teknik yang dapat memberikan keyakinan pada Bank.

Saat ini Bank menerapkan 2 (dua) faktor autentikasi *(two factor authentication)* untuk verifikasi transaksi keuangan yaitu melalui *user id* dan *password* serta instrumen elektronik yaitu *Hard Token* dalam melakukan transaksi finansial.

Syarat dan Ketentuan terkait layanan *Internet Banking* telah diatur pada saat Nasabah mendaftar sebagai pengguna Layanan *Internet Banking* yaitu terdapat pada Formulir Pendaftaran *Internet Banking-Perdania Direct*.

C. Internet BankingTransactional Activities

Customers can use Internet Banking services to obtain information and/or carry out banking transactions provided by the bank.

Following are services in Internet Banking :

1. Financial Transactions
2. Non-Financial Transactions

In financial transactions, Banks are required to ensure the suitability of the data and/or information used in Internet Banking. Compliance with the data and/or information used is carried out, among other things, through direct recording, verification of data sources, and techniques that can provide confidence to the bank.

Currently, the bank implements two authentication factors to verify financial transactions, namely user ID and password, as well as electronic instruments, namely hard tokens, to carry out financial transactions.

Terms and conditions related to Internet banking services are regulated when the customer registers as a user of the Internet Banking service, there is on the Internet Banking Registration Form.

D. Penanganan Pengaduan Nasabah Pengguna Internet Banking

Penanganan pertanyaan terkait layanan *Internet Banking* dapat disampaikan melalui IB *Helpdesk direct line* 021-5707278 pada hari dan jam operasional Bank, namun tidak terbatas selama 24 jam melalui email ib_helpdesk@perdania.co.id. Mekanisme penanganan terkait penggunaan *Internet Banking* telah diatur dalam SOP *Internet Banking.*

Untuk penanganan pengaduan Nasabah dapat disampaikan melalui petugas Bank / Kantor Cabang, *direct line* pengaduan (021) 5707300, atau fax (021) 5701936 pada hari dan jam operasional Bank, namun tidak terbatas selama 24 Jam melalui email cust-comm@perdania.co.id, yang mekanismenya agar mengacu kepada Kebijakan Pelayanan & Penyelesaian Pengaduan Nasabah & Penyelesaian Sengketa Intern.

E. Sistem Informasi Akuntansi

Sistem Informasi Akuntansi adalah suatu sistem yang dirancang untuk mengumpulkan, mengolah, menyimpan, mengintegrasikan, serta mengkomunikasikan data.

Internet Banking merupakan bagian dari Sistem Informasi Akuntansi yang melibatkan Nasabah dalam sistem pemrosesan transaksi yang terotomatisasi. Sistem pemrosesan transaksi yang tercatat kedalam sistem akan memberikan *output* berupa informasi yang diperlukan bagi Nasabah maupun Bank.

Berikut adalah jenis transaksi perbankan yang dapat dilakukan melalui *Internet Banking* :

1. Pengecekan Saldo
2. Pengecekan Status Transaksi
3. Pengecekan Status Deposito
4. Pemindahbukuan
5. Transfer (dalam Rupiah)
6. Transfer (dalam Valas)
7. Pembayaran Pajak Non-Import
8. Pembukaan Deposito

D. Handling Internet Banking Customer Complaints

Handling questions related to Internet Banking services can be submitted via the IB Helpdesk direct line at 021-5707278 on bank operational days and hours, but not limited to 24 hours, via email at ib_helpdesk@perdania.co.id . The handling mechanism related to the use of Internet banking has been regulated in the SOP Internet Banking.

For handling customer complaints, Customers can be submitted via bank / branch office officers, direct complaint line (021) 5707300, or fax (021) 5701936 on bank operational days and hours, but not limited to 24 hours, via email cust-comm@perdania.co.id, the mechanism of which refers to The Service and Settlement of Customer Complaints and Internal Dispute Resolution Policy.

E. Accounting Information System

Accounting information systems are systems designed to collect, process, store, integrate, and communicate data.

Internet banking is part of the Accounting Information System, which involves customers in an automatic transaction processing system. The transaction processing system recorded in the system will provide output in the form of information needed by the customer and the bank.

The following types of banking transactions can be carried out via Internet banking:

1. Balance Inquiry
2. Transaction History
3. Deposit Inquiry
4. Overbooking
5. Domestic Transfer
6. Remittance
7. Tax Payment
8. Deposit Placement

9. Transaksi Import & Ekspor

10. Pemesanan Buku Cek

11. Pendaftaran Penerima

12. Informasi Kurs.

Untuk aktivitas No. 1 – 9 terhubung dengan sistem *Core Banking* Bank, dimana transaksi yang dilakukan akan tercatat pada sistem akuntansi pembukuan Bank.

F. Kewajiban Pelaporan

1. Bank yang dalam penyelenggaraan layanan digital melakukan kerja sama dengan mitra Bank wajib menyampaikan daftar mitra Bank
2. Laporan realisasi penyelenggaraan Layanan Digital kepada Otoritas Jasa Keuangan

   Target: paling lama 5 (lima) hari kerja setelah implementasi bagi Bank yang telah memperoleh izin untuk menyelenggarakan Layanan Digital yang memenuhi kriteria produk baru;
3. Laporan evaluasi penyelenggaraan Layanan Digital yang memenuhi kriteria produk baru OJK

   Target: paling lama 3 (tiga) bulan setelah implementasi;

9. Trade Finance

10. Cheque Book Request

11. Beneficiary Registration

12. Rate Information

Activities 1–9 are connected to the bank's core banking system, where transactions carried out will be recorded in the bank's bookkeeping accounting system.

F. Reporting Obligations

1. Banks that collaborate with bank partners in providing digital services are required to submit a list of bank partners
2. Report on the realization of the implementation of Digital Services to the Financial Services Authority

   Target: no later than 5 (five) working days after implementation for Banks that have received permission to provide Digital Services that meet the new product criteria;
3. Evaluation report on the implementation of Digital Services that meet OJK's new product criteria

   Target: no later than 3 (three) months after implementation;

V. PENANGANAN PENYELENGGARAAN INTERNET BANKING DALAM KEADAAN GANGGUAN

A. Prosedur Tanggap Darurat

Bank harus memberikan pelayanan kepada Nasabah secara berkelanjutan ketika aplikasi *Internet Banking* sedang dalam gangguan.

Ketika sistem Internet Banking ini mengalami gangguan maka dapat berdampak besar terhadap aktivitas operasional Bank. Oleh karena itu Bank harus mempersiapkan rencana-rencana strategis untuk menghadapi kemungkinan buruk yang terjadi serta mengembalikan ke kondisi semula.

Prosedur tanggap darurat adalah prosedur yang harus segera dilakukan ketika terjadi gangguan pada aplikasi *Internet Banking*.

Suatu kondisi disebut sebagai kegagalan sistem apabila mengalami sedikitnya salah satu dari kejadian berikut :

a. Tidak dapat *log-in* ke dalam aplikasi dikarenakan system.
b. User tidak dapat melakukan input transaksi dikarenakan system.
c. Transaksi tidak dapat di *approved/released* dikarenakan system.
d. Aplikasi/sistem terhenti, *offline, error* dan lain sebagainya.
e. Masalah pada *Interface*.
f. Kondisi lainnya yang ditentukan oleh Divisi TI sebagai kegagalan sistem

Berikut prosedur tanggap darurat yang harus dilakukan :

1. Pihak yang mengetahui terjadinya gangguan baik dari Internal Bank maupun dari Nasabah harus segera menyampaikan laporan ke Divisi TI.
2. Kepala / Wakil Kepala Divisi TI memberi instruksi kepada IB *Helpdesk* untuk menyelidiki kondisi gangguan dan mencari solusi untuk menyelesaikan permasalahan.

V. HANDLING INTERNET BANKING IMPLEMENTATION UNDER DISRUPTION

A. Emergency Response Procedures

Banks must provide services to customers continuously when the Internet banking application is in disruption.

When the Internet banking system has disruption, it can have a major impact on the bank's operational activities. Therefore, the bank must prepare strategic plans to face the bad possibilities that occur and return to its original condition.

Emergency response procedures are procedures that should be carried out immediately when an interruption occurs in an Internet Banking application.

A condition is called a system failure when you experience at least one of the following:

a. Can’t Login to application due to the system.
b. Users can’t input transactions due to the system.
c. Transactions cannot be approved /released due to the system.
d. Application/system down, offline, errors and etc.
e. Interface Problem.
f. Other conditions determined by the Information Technology Division to constitute system failure

The Following are emergency response procedures must be carried out :

1. Parties who are aware of any disturbance either internally from the bank or from customers are required to immediately submit a report to the Information Technology Division
2. Head or Deputy Head of the Information Technology Division gives instructions to the IB Helpdesk to investigate the disturbance condition and find solutions to resolve the problem.

3. IB *Helpdesk* akan berkoordinasi dengan vendor terkait mengenai gangguan yang terjadi dan mencari solusi untuk menyelesaikan permasalahan.

4. Jika masalah tidak dapat diselesaikan dalam waktu 30 (tiga puluh) menit, maka Kepala/Wakil Kepala Divisi TI menginformasikan kepada Direktur TI dan Divisi terkait perihal gangguan yang terjadi dan mempertimbangkan waktu yang dibutuhkan untuk proses manual dan *Cut Off Time*.

   Pemberitahuan berisi informasi adanya gangguan pada aplikasi Internet Banking dan berkoordinasi dengan Divisi terkait untuk dapat membantu berkomunikasi dengan Nasabah.

5. Berdasarkan instruksi dari Kepala/Wakil Kepala Divisi TI, IB *Helpdesk* akan mengirimkan pemberitahuan ke Nasabah *Internet Banking* melalui aplikasi Mailblast yang berisi informasi adanya gangguan pada aplikasi *Internet Banking* dan menginformasikan bahwa untuk sementara waktu *Internet Banking* tidak dapat digunakan.

6. Ketika keadaan gangguan dinyatakan bersifat *major* maka Divisi TI akan berkoordinasi dengan Departemen *Corporate Secretary* untuk menyiapkan pengumuman / pemberitahuan ke Nasabah *Internet Banking* melalui aplikasi *Mailblast*.

B. Prosedur Penanganan Transaksi Internet Banking Selama Gangguan

Prosedur penanganan transaksi Internet Banking selama gangguan mengacu kepada SOP *Internet Banking Perdania Direct* terkait Penanganan Transaksi yang Gagal dikarenakan Kegagalan Sistem.

C. Prosedur Pemulihan Usaha

1. Jika gangguan telah selesai diperbaiki, maka langkah berikutnya adalah melakukan testing aplikasi berjalan dengan normal dengan melakukan tes di *development Internet Banking* atau di *production* dengan menggunakan *log-in test*.

2. Setelah uji coba berhasil, laporkan kepada Kepala / Wakil Kepala Divisi TI.

3. IB Helpdesk will coordinate with relevant vendors regarding the disruption that occurs and find solutions to resolve the problem.

4. If the problem cannot be resolved within 30 (thirty) minutes, then the Head/Deputy Head of the IT Division shall notify the Director of IT and the relevant Division regarding the disturbance that has occurred and consider the time required for the manual process and Cut Off Time

   This notification contains information about problems with the Internet Banking application and coordinates with related divisions to assist communication with customers.

5. Based on instructions from the Head/Deputy Head of the IT Division, IB Helpdesk will send a notification to Internet Banking customers via the Mailblast application containing information about problems with the Internet Banking application and informing them that Internet Banking cannot be used temporarily.

6. If the disruption is declared major, the IT Division will coordinate with the Corporate Secretary Department to prepare an announcement or notification to Internet banking customers via the Mailblast application.

B. Internet Banking Transactions Handling During Disturbances Procedures

Internet Banking transaction procedures during disruption refer to the SOP Perdania Direct Internet Banking regarding Handling Failed Transactions Due to System Failure.

C. Business Recovery Procedures

1. If the problem has been fixed, the next step is to test the application so that it runs normally by testing Internet banking development or in production using log-in testing.

2. After the test is successful, report it to the Head or Deputy Head of the IT Division.

3. Kepala/Wakil Kepala Divisi TI melaporkan kepada Direktur TI bahwa aplikasi *Internet Banking* sudah berjalan Normal.

4. Berdasarkan instruksi dari Direktur TI, Kepala/Wakil Kepala Divisi TI akan memberitahukan kepada Divisi terkait bahwa aplikasi *Internet Banking* sudah berjalan Normal.

5. Berdasarkan instruksi dari Direktur dan atau Kepala/Wakil Kepala Divisi TI, IB *Helpdesk* akan mengirimkan pemberitahuan ke Nasabah Internet Banking melalui aplikasi Mailblast yang berisi informasi adanya bahwa aplikasi Internet Banking sudah kembali Normal.

6. Berkoordinasi dengan Divisi Operasional memastikan transaksi yang terkena dampak gangguan telah diproses dengan benar.

D. Prosedur Laporan Insidentil ke OJK

Kewajiban Laporan dengan mengacu kepada ketentuan pelaporan insidentil sebagaimana tercantum dalam pasal 60 POJK No.11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum yaitu :

1. Dalam hal terjadi insiden Teknologi Informasi (TI) yang berpotensi dan/atau telah mengakibatkan kerugian yang signifikan dan/atau mengganggu kelancaran operasional Bank, Bank wajib menyampaikan:

   a. Notifikasi awal paling lama 24 jam setelah insiden TI diketahui; dan

   b. Laporan insiden TI paling lama 5 hari kerja setelah insiden TI diketahui.

2. Notifikasi awal sesuai ayat 1a disampaikan melalui sarana elektronik secara tertulis kepada OJK berdasarkan informasi awal yang tersedia.

3. Laporan insiden TI sesuai ayat 1b merupakan bagian dari laporan kondisi yang berpotensi menimbulkan kerugian yang signifikan terhadap kondisi keuangan Bank sesuai dengan POJK mengenai penerapan manajemen risiko bagi Bank Umum.

4. Dalam hal terdapat pengaturan otoritas lain mengenai penyampaian notifikasi awal

3. Head/Deputy Head of the IT Division reports to the Director of IT that the Internet Banking application is running normally.

4. Based on instructions from the Director of IT, the Head/Deputy Head of IT Division will notify the relevant Division that the Internet Banking application is running normally.

5. Based on instructions from the Director or Head/Deputy Head of the IT Division, the IB Helpdesk will send a notification to Internet Banking customers via the Mailblast application containing information that the Internet Banking application has returned to normal.

6. Coordinate with the Operations Division to ensure that transactions affected by disruptions have been processed correctly.

D. Incidental Reporting Procedures to OJK

Reporting Obligations with reference to incidental reporting provisions as stated in Article 60 of POJK No. 11/POJK.03/2022 concerning the Implementation of Information Technology by Commercial Banks,:

1. In the event that an information technology (IT) event occurs that has the potential to result in large losses and/or disrupts the smooth operation of the bank, the bank is obliged to report:

   a. Initial notification no later than 24 hours after the IT incident is discovered; and

   b. Reporting IT incidents no later than 5 working days after the IT incident is discovered.

2. The initial notification, as intended in paragraph 1a, is submitted via electronic means in writing to the OJK based on the initial information available.

3. The IT incident report in accordance with paragraph 1b is part of the condition report, which has the potential to cause significant losses to the bank's financial condition in accordance with POJK concerning the implementation of risk management for commercial banks.

4. In the event that there are other authority regulations regarding the delivery of initial

dan/atau laporan insiden TI dalam jangka waktu yang lebih cepat daripada jangka waktu sesuai ayat (1), Bank wajib menyampaikan notifikasi awal dan/atau laporan insiden TI kepada OJK pada saat yang bersamaan sesuai dengan ketentuan peraturan perundang-undangan otoritas lain dimaksud.

Bank yang telah menyampaikan notifikasi awal dan/atau laporan insiden TI sesuai ayat (4) dianggap telah memenuhi ketentuan sesuai ayat (1) huruf a dan/atau huruf b.

notification and/or IT incident reports within a period that is quicker than the period referred to in paragraph (1), the bank is obliged to provide initial notification. and/or IT incidents while reporting to OJK. in accordance with the provisions of the laws and regulations of other relevant authorities.

Banks that have submitted initial notification and/or IT incident reports in accordance with paragraph (4) are deemed to have fulfilled the provisions in accordance with paragraph (1), letters a and/or b.

Apabila terdapat gangguan dalam pemrosesan transaksi pembayaran agar mengacu pada ketentuan sebagaimana tercantum dalam Surat BI No.25/254/DSSK/Srt/Rhs tanggal 20Juni 2023 perihal Kewajiban Penyampaian Laporan Insidental. Laporan insidental dapat disampaikan melalui PIC yang ditunjuk. Dalam PBI No. 14/23/PBI/2012 tanggal 26 Desember 2012 tentang Transfer Dana (PBI TD) Bank wajib menyampaikan hal-hal sebagai berikut :

If there is a disruption in processing payment transactions, please refer to the provisions as stated in BI Letter No. 25/254/DSSK/Srt/Rhs dated June 20, 2023, concerning the obligation to submit incidental reports. Incidental reports can be submitted via the appointed PIC. In PBI No. 14/23/PBI/2012 dated December 26, 2012 concerning Fund Transfers (PBI TD), banks are required to convey the following :

1. Bank wajib menyampaikan laporan berkala dan laporan insidental.

2. Laporan insidental dimaksud antara lain terdiri atas laporan gangguan dalam pemrosesan transaksi pembayaran dan tindak lanjut yang telah dilakukan, dan laporan terjadinya keadaan kahar *(force majeure)* atas penyelenggaraan pemrosesan transaksi pembayaran.

3. Terjadinya gangguan dan keadaan kahar *(force majeure)* harus diberitahukan kepada Bank Indonesia paling lambat 1 (satu) jam setelah kejadian.

4. Penyampaian laporan gangguan wajib disampaikan paling lambat 3 (tiga) hari setelah kejadian, dan laporan keadaan kahar wajib disampaikan paling lambat 3 (tiga) hari kerja setelah kejadian.

5. Terkait dengan ketentuan pelaporan insidental dimaksud, apabila terjadi gangguan dalam pemrosesan transaksi pembayaran atau keadaan kahar, Bank wajib untuk memberitahukan dengan segera, maksimal 1 (satu) jam setelah kejadian yang dialami, melalui call centre Bank Indonesia dengan nomor telepon 131 atau emailn dengan alamat

1. Banks are required to submit periodic reports and incidental reports.

2. The incidental reports referred to include reports of disruptions to the payment transaction process and follow-up actions that have been carried out, as well as reports of force majeure circumstances regarding the implementation of the payment transaction process.

3. The occurrence of disruption and force majeure must be notified to Bank Indonesia no later than 1 (one) hour after the incident.

4. Submission of disturbance reports must be submitted no later than 3 (three) days afte the incident, and force majeure reports must be submitted no later than 3 (three) working days after the incident.

5. In connection with the incidental reporting provisions as intended, if there is a disruption in the payment transaction process or a force majeure situation, the Bank is obliged to notify you immediately, a maximum of 1 (one) hour after the incident occurs. , via the Bank Indonesia call center at telephone number 131 or via email at laporaninsidental@bi.go.id (ref: BI Letter

laporaninsidental@bi.go.id (ref: Surat BI No. 25 / 254/ DSSK/ Srt/Rhs tanggal 20 Juni 2023 perihal Kewajiban Penyampaian Laporan Insidental).

No. 25/254/DSSK/Srt/Rhs dated June 20, 2023 concerning the Obligation to Submit Incidental Reports).

VI. PENUTUP

Kebijakan *Internet Banking* 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 *Internet Banking* ini memasukan Pedoman Rencana Keberlangsungan Usaha Aplikasi *Internet Banking* yaitu terkait Penanganan Keadaan Tidak Normal atau Gangguan Dalam Penyelenggaraan *Internet Banking*.

Kebijakan *Internet Banking* ini mulai berlaku sejak memperoleh persetujuan Presiden Direktur pada tanggal 25 April 2024 dan Dewan Komisaris pada tanggal 7 Mei 2024 dan mencabut Kebijakan *Internet Banking,* Edisi 9, Januari 2023 dan menghapus Pedoman Rencana Keberlangsungan Usaha Aplikasi Internet Banking, Edisi 8, September 2023.

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

CLOSING

This Internet Banking policy is issued in 2 (two) languages, namely Indonesian and English, and if there are differences in interpretation between the two, then what is referred to is Indonesian.

This Internet Banking Policy contains Guidelines for Business Continuity Plans for Internet Banking Applications, namely regarding Handling Abnormal Conditions or Disruptions in the Implementation of Internet Banking.

This Internet Banking Policy effective after obtaining approval from the President Director on April 25, 2024 and the Board of Commissioners on May 7, 2024 and revoking the Internet Banking Policy, Edition 9, January 2023, and removing the Internet Banking Application Business Continuity Plan Guidelines, Edition 8, September 2023.

This policy will be reviewed at latest every 2 (two) years or if needed as an improvement effort following the business development and the need of Bank or following the changes of base regulation.