Bank Resona Perdania

KEBIJAKAN JARINGAN KOMUNIKASI
NETWORK COMMUNICATION POLICY

Edisi ke-6, November 2023

6th Edition, November 2023

BOD *Approval* No. 023/ITD/IT-PLN/I/2024

BOC *Approval* No. 024/BOC/II/2024-ITD/IT-PLN

DAFTAR ISI
Table of Content

Hal/*Page*

Bank Resona Perdania

I. PENDAHULUAN

A. Latar Belakang

Untuk memenuhi kebutuhan bisnis perusahaan dengan kinerja jaringan yang baik, aman, dan dengan tingkat kontrol yang tinggi.

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.

   Pasal 40 & 41 dicabut oleh PERPU No. 1 thn 2017 tentang Akses Informasi Keuangan Untuk Kepentingan Perpajakan.

   Beberapa pasal dicabut oleh UU RI No.4 Tahun 2023 tentang Penyelenggaraan Produk Bank Umum.

2. 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 No.18/POJK.03/2016 ini dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam POJK No.17 Tahun 2023 tentang Penerapan Tata Kelola Bagi Bank Umum.

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

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

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

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

I. INTRODUCTION

A. Background

To fulfill business plan that supported by reliable network performance, secure and high level control.

B. Reference

1. Law of the Republic of Indonesia No. 7 of 1992, as amended by Law of the Republic of Indonesia No. 10 of 1998 concerning banking.

   Articles 40 and 41 were revoked by PERPU No. 1 of 2017 concerning access to financial information for tax purposes.

   Several articles were revoked by Law of the Republic of Indonesia No. 4 of 2023 concerning the implementation of commercial bank products.

2. POJK No.18/POJK.03/2016 concerning Implementation of Risk Management for Commercial Banks.

   Since October 30, 2021, Articles 20, 21, 22, and 24 in POJK No. 18/POJK.03/2016 concerning the Implementation of Risk Management for Commercial Banks have been declared revoked and no longer valid based on POJK No. 13/POJK.03/2021 concerning the Application of Commercial Bank Products.

   POJK No.18/POJK.03/2016 is declared still valid as long as it does not conflict with the provisions in POJK No.17 of 2023 concerning the Implementation of Governance for Commercial Banks..

3. SEOJK No. 34/SEOJK.03/2016 dated 1 September 2016 concerning the Implementation of Risk Management for Commercial Banks.

4. POJK No.11/POJK.03/2022 concerning the Implementation of Information Technology by Commercial Banks;

5. SEOJK No. 21 /SEOJK.03/2017 dated June 6, 2017 about Implementation of Risk Management in the use of Information Technology by Public Bank.

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

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

7. POJK No.6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan;
   a. Semua peraturan pelaksana dari POJK No.1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan; dan
   b. Ketentuan-ketentuan pelaksana yang mengatur Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan, dinyatakan tetap berlaku sepanjang tidak bertentangan dengan POJK ini.
   c. POJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan dan ketentuan pelaksanaan mengenai kerahasiaan data dan keamanan data dan/atau informasi pribadi konsumen;
   d. Pasal 32 POJK No.76/POJK.07/2016 tentang Peningkatan Literasi dan Inklusi Keuangan di Sektor Jasa Keuangan bagi Konsumen dan/atau Masyarakat; dan
   e. PBI No.7/6/PBI/2005 tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah dicabut dan dinyatakan tidak berlaku.

8. SEOJK No.24/SEOJK.03/2023 Tentang Penilaian Tingkat Maturitas Digital Bank Umum.

9. PBI No.3 Tahun 2023 Perlindungan Konsumen Bank Indonesia ;

   Pada saat PBI ini mulai berlaku, semua peraturan yang merupakan peraturan pelaksanaan dari PBI No.22/20/PBI/2020 tentang Perlindungan Konsumen Bank dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam Peraturan Bank Indonesia ini.

10. POJK No. 18/POJK.07/2018 tentang Layanan Pengaduan Konsumen Sektor Jasa Keuangan.

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

7. POJK No.6/POJK.07/2022 concerning Consumer and Public Protection in the Financial Services Sector :
   a. All implementing regulations from POJK No.1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector; and
   b. The implementing provisions governing Consumer and Public Protection in the Financial Services Sector are declared to remain in effect as long as they do not conflict with this POJK.
   c. POJK Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector and implementing provisions regarding data confidentiality and security of consumer data and/or personal information.
   d. Article 32 POJK No.76/POJK.07/2016 concerning Increasing Literacy and Financial Inclusion in the Financial Services Sector for Consumers and/or the Community; and
   e. PBI No.7/6/PBI/2005 concerning Transparency of Bank Product Information and Use of Customer Personal Data is revoked and declared no longer valid.

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

9. PBI No. 3 of 2023 Bank Indonesia Consumer Protection;

   When this PBI comes into force, all regulations that are implementing regulations of PBI No. 22/20/PBI/2020 concerning Bank Consumer Protection are declared to still be valid as long as they do not conflict with the provisions of this Bank Indonesia Regulation.

10. POJK No.18/POJK.07/2018 about concerning Financial Services Sector Consumer Complaints Services

11. Kebijakan Tingkat Otorisasi	11. Levelling Authority Policy
12. Kebijakan Tugas dan Wewenang	12. Duties and Authorities Policy
13. Kebijakan *Job Description*	13. Job Description Policy
14. Kebijakan Manajemen Risiko Secara Umum (Individual)	14. General Risk Management Policy (Individual)
15. Kebijakan Manajemen Risiko Teknologi Informasi	15. Information Technology Risk Management Policy
16. Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem Dalam Penggunaan Teknologi Informasi	16. Information Security and System Risk Management in the Use of Information Technology Policy.
17. Kebijakan Pengawasan Keamanan Sistem & Informasi	17. System and Information Security Monitoring Policy
18. Pedoman *Business Continuity Plan* Sistem *Core Banking*	18. Business Continuity Plan of Sistem Core Banking Guidelines
19. Pedoman Rencana Kelangsungan Usaha Aplikasi *Internet Banking*	19. Business Continuity Plan Internet Banking Application Guidelines
20. Kebijakan Pengelolaan *Website*	20. Website Management Policy
21. Kebijakan *Antivirus*	21. Antivirus Policy
22. Kebijakan Manajemen Risiko Operasional	22. Operational Risk Management Policy
23. Kebijakan *Business Continuity Plan* Aplikasi SKNBI	23. Business Continuity Plan of SKNBI Policy
24. Kebijakan *Business Continuity Plan* Aplikasi BI-RTGS	24. Business Continuity Plan of RTGS Policy
25. Kebijakan *Business Continuity Plan* Aplikasi Sistem Operasional	25. Business Continuity Plan of Operational System Policy
26. Kebijakan Komite Pengarah Teknologi Informasi	26. IT Steering Committee Policy
C. Tujuan	**C. Purpose**
1. Memastikan bahwa integritas jaringan dipelihara.	1. Ensure that network integrity is maintained.
2. Memaksimalkan kinerja jaringan.	2. Maximize network performance.
3. Memastikan pengelolaan, penggunaan, pengawasan / kontrol, keamanan jaringan dilakukan secara maksimal.	3. Ensure that network management, use, monitoring/control and network security are carried out optimally
4. Meminimalkan kemungkinan risiko terkait penggunaan jaringan.	4. Minimize possible risks related to network use

D. Ruang Lingkup

1. Keamanan

   Jaringan harus dirancang, dikonfigurasi dan mempunyai tingkat kontrol yang tinggi untuk melindungi Bank dari risiko yang mungkin terjadi (internal dan/atau eksternal). Keamanan jaringan dilakukan untuk memastikan ketersediaan, kehandalan dan tingkat kerahasiaan jaringan.

2. Ketersediaan

   Bank harus meyakini bahwa ketersediaan jaringan yang digunakan untuk sistem operasional dan pelayanan nasabah (*high risk*) mempunyai jaringan *backup*. Jika terjadi gangguan terhadap jaringan, Bank harus mempertimbangkan penanganan selanjutnya berdasarkan Kebijakan BCP dan / atau Pedoman dari sistem yang terpengaruh.

3. Kerahasiaan

   Untuk menghindari risiko terkait jaringan, konfigurasi dan akses ke dalam jaringan harus dibatasi hanya untuk staff yang berhak dan/atau vendor terkait.

4. Penggunaan

   Segala penggunaan jaringan di lingkungan internal Bank dan yang terkoneksi dari luar ke dalam jaringan Bank diatur dalam prosedur-prosedur untuk meminimalkan kemungkinan risiko terkait jaringan.

5. Penanganan Masalah

   Setiap penanganan masalah terkait jaringan harus sesuai dengan prosedur dan di dokumentasikan agar ketika masalah yang sama terjadi akan lebih cepat dalam penyelesaiannya.

6. Jenis Jaringan

   Terdapat dua jenis jaringan di Bank Resona Perdania, yaitu Jaringan menggunakan kabel data dan jaringan tanpa kabel (nirkabel/wifi).

D. Scope

1. Security

   The network must be designed, configured and have a high level of control to protect the Bank from possible risks (internal and/or external). Network security is carried out to ensure the availability, reliability and level of network confidentiality.

2. Availability

   Banks must ensure that the network used for operational systems and customer service (high risk) has a backup network. If network disruption occurs, the Bank must consider further treatment based on the BCP Policy and/or Guidelines for the affected system.

3. Confidentiality

   To avoid network related risk, configuration and access to the network should be limited to authorized staff and/or associated vendors

4. Usage

   All network usage within the Bank's internal environment and those connected from outside to the Bank's network are regulated by procedures to minimize possible risks related to the network.

5. Problem Handling

   Handling of network related problems must be in accordance with procedures and documented so that if the same problem occurs it will be resolved more quickly.

6. Network Type

   There is two types of networks at Bank Resona Perdania, that is network use cable and wireless network (wifi).

II. PERAN DAN TANGGUNG JAWAB

A. Manajemen

1. Memastikan adanya pengawasan yang memadai terkait jaringan, baik kegiatan operasional, pengembangan, dan modifikasi.
2. Mempertimbangkan kebutuhan jaringan yang sesuai dengan kondisi bisnis dan strategi yang akan dikembangkan.
3. Memberikan persetujuan jika jaringan akan terkoneksi dengan pihak ketiga, berdasarkan analisa dan diskusi dengan *IT Steering Committee.*
4. Menetapkan prosedur dan kebijakan terkait jaringan agar kontrol terhadap jaringan dapat dilakukan dengan baik, efisien dan keamanan terjamin.
5. Menunjuk administrator (staf Divisi Teknologi Informasi) yang berkualifikasi untuk bertanggung jawab terhadap pengembangan jaringan, ketersediaan, keamanan dan kebutuhan jaringan. Staf tersebut akan berkoordinasi dengan Departemen Keamanan Informasi dan Kontrol Risiko Sistem.

B. Divisi Teknologi Informasi

1. Bertanggung jawab terhadap pemasangan untuk akses pengguna jaringan, pengamanan jaringan, konfigurasi, pemeliharaan dan kinerja jaringan dalam mengolah data, terutama jaringan yang digunakan pada aplikasi kritikal untuk mengantisipasi kemungkinan serangan dan gangguan terkait jaringan serta untuk memastikan jaringan sudah memenuhi standar keamanan yang telah ditentukan.
2. Melakukan kontrol aktifitas jaringan, akses, monitoring jaringan serta pengujian terhadap jaringan *backup* yang dilakukan secara berkala.
3. Melakukan pemeliharaan terhadap dokumentasi jaringan, termasuk *network address list* (IP *Address*) dan bertanggung jawab terhadap perubahan datanya.

II. JOB AND RESPONSIBILITY

A. Management

1. Ensure there is satisfy Network monitoring for operations, development and modification.
2. Consider network requirement which is inline with business condition and business plan.
3. Approve if the network will be connected to third party based on analysis and discussion with IT Steering Committee.
4. Define procedure and policy related Network so monitoring of Network can be run well, efficiently and secure.
5. Assign administrator (Information Technology Division Staff) who qualified to be responsible od Network development, security, and Network requirement then coordinate with Information Security and System Risk Control Department.

B. Information Technology Division

1. Responsible for installation of network user access, network security, configuration, maintenance and network performance in processing data, especially network that used by critical application, in order to anticipate potential attack and disturbance to network, also to make sure that the network already meets security standards.
2. Controlling network activity, access, network monitoring and network backup testing periodically.
3. Maintain of network documentation, including a list of network address (IP Address) and be responsible for data changes.

4. Melakukan tindakan ketika jaringan tidak berfungsi, dalam keadaan darurat atau terjadi penyusupan / serangan pada jaringan.

4. Take action when the network is not functioning, in an emergency or there is an intrusion/attack on the network.

5. Untuk menghindari kerusakan yang tidak disengaja sehingga dapat mengganggu proses operasional maka proses pemeliharaan jaringan harus dilakukan oleh orang yang berkualifikasi serta bertanggung jawab untuk menginstall dan memelihara perangkat jaringan secara rutin serta bertanggung jawab mengawasi proses *maintenance* jaringan yang dilakukan oleh *vendor*.

5. To avoid accidental damage that could disrupt operational processes, the network maintenance process must be carried out by a qualified person who is responsible for installing and maintaining network equipment on a regular basis and is responsible for supervising the network maintenance process by vendor.

6. Menginstall perangkat pengamanan jaringan pada setiap Komputer atau Laptop.

6. Install network security software at every computer or laptop.

7. Memastikan bahwa jaringan komunikasi yang dikelola oleh pihak ketiga memiliki peralatan jaringan dan jasa yang memadai.

7. Ensure that communications networks managed by third parties have adequate network equipment and services.

C. Departemen Keamanan Informasi dan Kontrol Risiko Sistem

C. Information Security and System Risk Control Department

1. Memastikan bahwa Kebijakan Jaringan Komunikasi sudah di implementasikan dan dilaksanakan sesuai dengan ketentuan.

1. Ensure that the Communication Network Policy has been implemented according to the provisions.

2. Melakukan pengawasan, pemantauan, peninjauan dan memberikan rekomendasi kepada Divisi Teknologi Informasi mengenai efektifitas penggunaan jaringan berdasarkan data dan laporan hasil uji coba jaringan dari Divisi Teknologi Informasi.

2. Supervise, monitor, review and provide recommendations to the Information Technology Division regarding the effectiveness of network use based on data and network test results reports from the Information Technology Division.

3. Melakukan pengawasan / pemantauan terhadap setiap perubahan / *upgrade* pada perangkat keras/perangkat lunak terkait jaringan dan memastikan bahwa proses tersebut telah berjalan sebagaimana mestinya.

3. Supervise / monitor any changes / improvements to hardware/software related to the network and ensure the process runs as it should.

4. Melakukan pemeriksaan dan *monitoring* secara berkala terhadap pengaturan parameter, *log* dan /atau audit *trail* pada perangkat jaringan terkait akses jaringan.

4. Regular inspection and monitoring of parameter settings, logs and/or audit trails on Network devices related to network access.

5. Melakukan pemantauan terhadap masalah/problem/kelemahan yang terjadi pada jaringan, baik internal maupun eksternal yang berkaitan dengan keamanan dan kebijakan.
6. Melakukan sosialisasi atau pemberitahuan ke *user* mengenai penggunaan jaringan, pengamanan jaringan, dan sistem komunikasi dalam keadaan darurat.

5. Monitoring network problem or weakness, both internal or external which is related to security and policy.
6. Conduct socialization or notification to users regarding network, security and communication systems in emergency situations.

D. *User*

1. Dilarang menggunakan / mengakses jaringan selain dari yang telah disediakan untuknya, kecuali dengan ijin dari Kepala Divisi Teknologi Informasi dan Departemen Keamanan Informasi dan Kontrol Risiko Sistem. Misalnya menggunakan *socket* jaringan yang tidak/belum digunakan (*idle*) agar dapat terhubung dengan jaringan internal.
2. Bertanggung jawab dalam menggunakan jaringan, baik dalam menggunakan internet, jaringan yang digunakan untuk lalu lintas data, dan lain-lain.

D. User

1. Prohibited to use / access networks other than those provided, except with permission from the Head of Information Technology Division and Information Security and System Risk Control Department. For example, using a network socket that is not/has not been used (idle) to connect to the internal network.
2. Responsible for network use, both in internet use, networks used for data traffic, etc.

E. Pihak Ketiga

1. Pihak ketiga yang akan menggunakan jaringan internal dalam rangka perbaikan /perawatan/ instalasi dan pengujian harus mendapatkan persetujuan terlebih dahulu dari Kepala Divisi Teknologi Informasi dan dan Departemen Keamanan Informasi dan Kontrol Risiko Sistem yang diajukan melalui Intramart
2. Akses jaringan oleh pihak ketiga terbatas hanya untuk jaringan yang dibutuhkan dan tidak diperkenankan melakukan akses di luar yang telah ditentukan, kecuali ditentukan lain (misalnya untuk kepentingan audit).
3. Akses jaringan ini hendaknya hanya bersifat sementara dan segera ditutup / diblokir apabila sudah selesai digunakan.

E. Third Party

1. Third parties who will use the internal network for repairs/maintenance/installation and testing must obtain prior approval from the Head of the Information Technology Division and Information Security and System Risk Control Department submitted by Intramart
2. Network access by third parties is limited to the required network and access outside that has been determined is not permitted, unless otherwise specified (for example for audit purposes).
3. Access to this network is only temporary and will be closed/blocked immediately after finished.

III. KEBIJAKAN DAN PROSEDUR

A. Pengukuran Kinerja dan Perencanaan Kapasitas Jaringan

1. Jaringan harus dapat diukur kinerjanya dengan menggunakan aplikasi *monitoring* jaringan atau dengan meminta bantuan vendor. Laporan *monitoring* jaringan dapat digunakan untuk rencana pengembangan jaringan di masa mendatang.
2. Divisi Teknologi Informasi melakukan pengukuran kinerja jaringan dan perencanaan kapasitas jaringan berdasarkan kebutuhan bisnis Bank.

B. Pengamanan Jaringan Komunikasi

1. Pengendalian Akses

   a. Pengamanan Fisik

      i. Perangkat jaringan ditempatkan pada lokasi yang aman dari gangguan dan terkunci.

      ii. Pemberian izin penggunaan/ akses fisik hanya untuk orang yang berwenang untuk melindungi dari kerugian disengaja atau tidak disengaja.

      iii. Kabel jaringan yang tidak digunakan harus dicatat dan ditutup aksesnya dari pihak yang tidak berhak.

      iv. Jaringan untuk lingkungan produksi sedapat mungkin terpisah dari jaringan pada lingkungan pengembangan (development), agar meminimalisasi kesalahan.

   b. Pengamanan Logik

      i. Kontrol akses logik dirancang untuk membatasi akses sistem, program dan file hanya untuk user yang sah, misalnya mengharuskan *use* untuk memasukkan *User* ID dan *password*.

      ii. Perangkat jaringan komunikasi harus dilengkapi dengan jaringan, misalnya firewall, IPS (Intrusion Prevention System), IDS (Intrusion Detection System), fortigate untuk pembatasan akses informasi, aplikasi monitoring jaringan, dan lain- lain.

III. POLICY AND PROCEDURE

A. Performance Assessment and Network Capacity Plan

1. Network performance must be able to be measured using a network monitoring application or by asking the vendor for help. Network monitoring reports can be used for future network development plans.
2. Information Technology Division measures network performance and plans network capacity based on the Bank's business needs.

B. Network Communication Security

1. Access Control

   a. Physical Security

      i. Network devices are placed in a location that is safe from interference and locked.

      ii. Permit physical use/access only to authorized persons to protect against intentional or unintentional harm.

      iii. Unused network cables must be logged and closed to unauthorized parties.

      iv. Networks for production environments are as separated as possible from networks in development environments, to minimize errors.

   b. Logical Security

      i. Logical access controls are designed to limit system, program, and file access to only authorized users, for example requiring users to enter a User ID and password.

      ii. Communication network devices must be equipped with networks, for example firewalls, IPS (Intrusion Prevention System), IDS (Intrusion Detection System), fortigate for limiting information access, network monitoring applications, etc.

iii. Untuk mengantisipasi gangguan pada jaringan serta meminimalisasi potensi serangan, maka diterapkanpemisahan / segmentasi berdasarkan pada *group server*, *group* lantai dan group Divisi.

iv. Setiap penambahan / perubahan terhadap pengaturan perangkat pengamanan harus mendapat persetujuan terlebih dahulu dari *Director in charge*, Kepala Divisi Teknologi Informasi dan Departemen Keamanan Informasi dan Kontrol Risiko Sistem.

iii. To anticipate disruptions to the network and minimize potential attacks, separation/segmentation is carried out based on server groups, floor groups and division groups.

iv. Any additions/changes to security device settings must obtain prior approval from the Director in Charge, Head of the Information Technology Division and the Information Security and System Risk Control Department.

2. Desain Jaringan Komunikasi

a. Topologi jaringan

Pemilihan topologi jaringan didasarkan pada letak geografis, skala jaringan, biaya, tujuan, kualitas kontrol, serta kecepatan pengiriman dan data.

b. Perencanaan kapasitas

Melakukan analisa *cost and benefit.*

2. Design of Network Communication

a. Network topology

Selection of network topology is based on geographic, network scale, cost, purpose, control quality, also for data transfer speed.

b. Capacity plan

Conduct cost and benefit analysis.

3. Kontrol Akses Jaringan

a. Divisi Teknologi Informasi bertanggung jawab dalam mengontrol, mengamankan dan mencegah akses yang tidak berhak ke dalam perangkat jaringan dan akses data melalui jaringan.

b. Divisi Teknologi Informasi dengan sepengetahuan Departemen Keamanan Informasi dan Kontrol Risiko Sistem mengatur akses terhadap computer atau laptop, sistem informasi, dan peralatan lainnya dibatasi hanya untuk authorize user.

c. Departemen Keamanan Informasi dan Kontrol Risiko Sistem melakukan review/monitoring, berdasarkan log user serta log akses fisik untuk memastikan bahwa hanya authorize user melakukan akses ke jaringan dan/atau perangkat

d. Masing-masing Kepala Departemen / Divisi / Cabang mengatur dengan tepat dan seksama mengenai User ID, hak akses apa saja yang diberikan, data / informasi mana saja yang bisa diakses, serta kemampuan apa saja yang diberikan (menghapus, merubah, atau menambah data).

3. Network Access Control

a. Information Technology Division is responsible for controlling, securing and preventing unauthorized access to network devices and data access over the network.

b. Information Technology Division, with the acknowledge of Information Security and System Risk Control Department, regulates that access to computers or laptop, information systems, and other equipment is limited to authorized users only.

c. Information Security and System Risk Control Department monitoring/review based on user logs and physical access logs, to ensure that only authorized users are accessing the network and/or devices.

d. Each Head of Department /Division /Branch precisely and carefully regulates the User ID, what access rights are given, what data/information can be accessed, and what capabilities are given (delete, change or add data).

e. Divisi Teknologi Informasi mempunyai dokumentasi yang jelas untuk setiap perubahan / modifikasi dalam jaringan termasuk perubahan hak akses dari setiap pemakai jaringan sehingga pengembangan jaringan dapat dilakukan melalui hasil analisa data yang ada.

f. Setiap penambahan / perubahan terhadap akses jaringan dan pengaturan parameter perangkat pengamanan harus melalui mekanisme yang berlaku dan dilaporkan kepada Director in Charge, Kepala Divisi Teknologi Informasi dan Departemen Keamanan Informasi dan Kontrol Risiko Sistem.

g. Setiap akses langsung ke perangkat komunikasi harus disetujui oleh Divisi Teknologi Informasi dan Departemen Keamanan Informasi dan Kontrol Risiko Sistem, dan pelaksanaannya diawasi oleh Staf Divisi Teknologi Informasi.

h. Setiap akses data yang menggunakan jaringan khusus atau umum diharuskan menggunakan jaringan yang aman, password, atau enkripsi.

4. *Remote* Akses

a. *Remote* akses adalah proses akses informasi dari luar perusahaan dengan menggunakan sarana *dial up/leased line*, termasuk akses yang dilakukan melalui VPN (*Virtual Private Network*), IP VPN, *IPSec*, *TCP Dial-up* dan melalui koneksi *Internet.*

b. Remote akses ke dalam jaringan Bank melalui VPN harus mendapat persetujuan dari Direktur yang membawahi *User* tersebut dan Kepala Divisi Teknologi Informasi dan Direktur yang membawahi Divisi Teknologi Informasi.

c. Remote akses kedalam jaringan Bank melalui koneksi internet harus di damping oleh staf Divisi Teknologi Informasi.

d. Lalu lintas data melalui *remote* akses harus menggunakan teknik otentikasi, enkripsi dan deskripsi, atau menggunakan *password.*

e. Information Technology Division has documentation of each changes / modification including changes to the access rights of each network user so that network development can be carried out through the results of existing data analysis.

f. Each addition/modification network access parameter settings and security devices must go through the applicable mechanism and be reported to the Director in Charge, Head of the Information Technology Division and the Information Security and System Risk Control Department

g. Direct access to communications devices must be approved by Information Technology Division and Information Security and System Risk Control Department, and implementation is supervised by Information Technology Division Staff.

h. Any data access using a special or public network must use a secure network, password or encryption.

4. Remote Access

a. Remote access is the process of accessing information from outside the company using a dial-up or leased line, including access through a VPN (Virtual Private Network), IP VPN, IPSec, TCP dial-up, and via an Internet connection.

b. Remote access to Bank's Network using VPN must be approve by Director incharge of user and Head of Information Technology Division and Director incharge of Information Technology Division

c. Remote access to Bank's Network using internet connection must be accompanied by Information Technology Staff.

d. Data traffic through remote access must use authentication, encryption, and decryption techniques, or passwords..

e. Setelah remote akses selesai dilakukan maka Divisi Teknologi Informasi harus segera menutup akses ke dalam jaringan/data.

f. Divisi Teknologi Informasi harus memastikan bahwa perangkat pengamanan jaringan aktif ketika *user* melakukan *remote* akses.

g. Divisi Teknologi Informasi bertanggung jawab untuk menyiapkan *user* dan *password* untuk akses informasi perusahaan.

5. Operasional dan Pemeliharaan Jaringan Komunikasi

a. Divisi Teknologi Informasi menyiapkan sarana *backup* dan *recovery* komunikasi yang memadai dan telah diuji coba secara berkala untuk menjamin kelangsungan operasional Bank.

b. Semua *software* dan aplikasi memerlukan *update* secara periodik. *Patch* yang baru harus diuji terlebih dahulu pada unit uji coba dan berhasil dengan baik, sebelum di implementasikan pada unit produksi, sesuai dengan mekanisme prosedur perubahan yang berlaku.

6. Audit *Trail*

a. Audit *trail* hendaknya dapat merekam semua kejadian termasuk perubahan pada *setting parameter*, hak akses perangkat jaringan serta penggunaannya.

b. Departemen Keamanan Informasi dan Kontrol Risiko Sistem secara teratur memeriksa laporan audit *trail* untuk *logging*, akses yang tidak sah dan statusnya (sukses atau gagal).

c. Audit *log* sekurang-kurangnya disimpan untuk 60 hari.

C. *Monitoring* Akses Jaringan

Monitoring akses jaringan dan/atau perangkat jaringan yang digunakan untuk sistem operasional dan pelayanan nasabah (*high risk*) dilakukan setiap hari.

D. Penggunaan Jaringan

Ruang lingkup peraturan ini meliputi untuk semua pengguna Internet di Bank Resona Perdania, baik untuk Dewan Komisaris, Direksi, karyawan, dan *vendor*.

e. Once remote access is complete, Information Technology Division must immediately close access to the network.

f. Information Technology Division must ensure that network security devices are active when users make remote access.

g. Information Technology Division is responsible for setting up users and passwords for accessing corporate information.

5. Operational and Maintenance of Network Communication.

a. Information Technology Division prepare an adequate network for backup and recovery that is tested on regular basis in orderto ensure bank business continuity.

b. Software and application are updated periodically. New patch is tested on development unit before implement it in the production unit, following procedure.

6. Audit Trail

a. Audit trail should record all activity include modify of parameter setting, access right and usage of network device.

b. Information Security and System Risk Control Department regular basis check audit trail report for logging, unauthorized access and its status (success or fail).

c. Audit log is keep at least 60days.

C. Network Access Monitoring

Monitoring of network access and/or network devices used for system operations and customer service (high risk) is carried out every day.

D. Network Usage

Scope of this regulation covers all Internet users at Bank Resona Perdania, including the Board of Commissioners, Directors, employees and vendors.

Semua aktivitas terkait jaringan harus dimonitor dan yang terkait penggunaan remote akses melalui koneksi internet tercatat pada buku *register*.

1. *Intranet*

   a. Seluruh karyawan dilarang menggunakan *web browser* diluar dari kepentingan kantor. Hal ini dimaksudkan untuk menghindari *virus, trojan*, dan perangkat lunak pengganggu/perusak lainnya. Virus dan sejenisnya dapat melakukan penetrasi terhadap pertahanan yang diaktifkan melalui *web browser*.

   b. Penggunaan aplikasi dengan fasilitas akses melalui *web browser* sedapat mungkin menggunakan proses autentikasi/verifikasi yaitu dengan menggunakan *User ID* dan *password*.

2. *Website*

   a. *Website* merupakan sarana yang sangat penting dalam memasarkan produk dan sekaligus sebagai sumber informasi yang penting bagi perusahaan.

   b. Divisi Teknologi Informasi bertanggung jawab untuk memilih vendor yang berkualitas untuk pembuatan *website*, pengembangan dan pemeliharaan berdasarkan Izin Direksi.

   c. *Website* di *update* berdasarkan Kebijakan Pengelolaan *Website* dan setiap proses *update* yang dilakukan harus didokumentasikan dan di*review* secara berkala.

   d. Karyawan yang ditunjuk atau telah mendapatkan tugas / wewenang untuk melakukan proses update informasi pada *website* harus bertanggung jawab terhadap kebenaran dan keaslian informasi yang dimasukkan ke dalam *website.*

   e. Informasi yang ada dalam *website* harus dijaga dari kemungkinan pencurian data meskipun sedang dalam proses pemeliharaan.

All network related activities are monitored and stored in a log book or register, which will be reviewed periodically and will be used if necessary.

1. Intranet

   a. All employees are prohibited from using web browsers outside the interests of the office. It is intended to avoid viruses, trojans, and other intrusive / malicious software. Viruses and the like can penetrate the defences activated through web browsers.

   b. Use of the application with access facilities through the web browser as far as possible using the authentication/verification process i.e. using the User ID and password.

2. Website

   a. Website is a very important in the marketing of products and as an important source of information for the company.

   b. Information Technology Division is responsible for selecting qualified vendors for website creation, development and maintenance based on BoD approval.

   c. Website update base on Website Management Policy and each update process is documented and reviewed periodically.

   d. Website officers in charge of updating website information are responsible for the truth and authenticity of the information on the website

   e. Information on the website must be protected from the data theft even though it is under maintenance

f. Divisi Teknologi Informasi bertanggung jawab untuk melakukan *backup* terhadap *website* secara keseluruhan termasuk *database*nya secara berkala guna mengantisipasi terjadinya serangan terhadap *website* (misalnya *re-routing address*, *defacing* terhadap tampilan, dan lain-lain), agar proses pemulihan terhadap *website* dapat dilakukan sesegera mungkin dan meminimalisasi resiko dengan tersedianya *backup* tersebut.

f. Information Technology Division responsible for periodically backup website include the database to anticipate website attack (such as re-routing address, interface deface, and other) so the restoration is immediate and to minimize risk.

E. *Voice over Internet Protocol* (VoIP)

Adalah teknologi yang mampu melewatkan trafik suara, video dan data yang berbentuk paket melalui jaringan *IP*. Jaringan *IP* sendiri adalah merupakan jaringan komunikasi data yang berbasis *packet-switch*, jadi dalam bertelepon menggunakan jaringan *IP* atau *Internet.*

E. Voice over Internet Protocol (VoIP)

Is a technology that is capable of passing voice, video and data traffic in packet form over an IP network. The IP network itself is a packet-switch based data communications network, so that when making telephone calls you use an IP network or the Internet.

1. Pengawasan Penggunaan VoIP

   a. Untuk menjaga kelancaran lalulintas data, penggunaan *VoIP* hanya diperuntukan untuk kepentingan perusahaan/pekerjaan.

   b. Divisi Teknologi Informasi bertanggung jawab untuk memonitor penggunaan *VoIP* dengan membandingkan antar *user*, jumlah akses data, dan kapasitas *bandwidth.*

   c. Apabila jumlah pengguna semakin meningkat, maka Divisi Teknologi Informasi harus membuat analisa terhadap penggunaan/traffic tersebut, apakah perlu dilakukan upgrade terhadap bandwidth atau langkah lainnya tersebut agar masalah tersebut dapat diatasi.

1. Supervision for VoIP Usage

   a. To maintain smooth data traffic, the use of VoIP is only for the company or business

   b. Information Technology Division is responsible to monitor VoIP usage by comparing user, access data and bandwidth capacity.

   c. If user increases, then Information Technology Division should make analysis of traffic use, whether needs to upgrade or take other step to handle the problem.

2. Pengawasan Oleh Divisi Teknologi Informasi/Vendor

   a. Divisi Teknologi Informasi bertanggung jawab untuk melakukan pengaturan *bandwidth* akses data dan penggunaan *VoIP.*

   b. Divisi Teknologi Informasi /vendor bertanggung jawab melakukan setting IP address untuk menghindari konflik penggunaan jaringan VoIP.

   c. Divisi Teknologi Informasi akan memberikan laporan kepada Departemen Keamanan Informasi dan Kontrol Risiko Sistem Informasi dan Kontrol Risiko Sistem berkaitan dengan kinerja jaringan.

2. Supervision by Information Technology Division / Vendor

   a. Information Technology Division is responsible to setting access bandwidth and VoIP usage.

   b. Information Technology Division / Vendor is responsible to setting IP address to prevent IP conflict

   c. Information Technology Division submit report of network performance to Information Security and System Risk Control Departmentand System Risk Controller Department.

F. Prosedur Penanganan Masalah

1. Apabila terjadi gangguan jaringan atau serangan jaringan komunikasi, maka user yang pertama kali mengetahui adanya gangguan tersebut, harus segera menginformasikan ke Kepala Divisi/ Departemen/ Cabang terkait, Kepala Divisi Teknologi Informasi, dan Departemen Keamanan Informasi dan Kontrol Risiko Sistem Informasi dan Kontrol Risiko Sistem.
2. Kepala Divisi Teknologi Informasi dan Departemen Keamanan Informasi dan Kontrol Risiko Sistem melakukan koordinasi untuk melakukan pencegahan dan penanganannya. Misalnya memutus jaringan komunikasi atau menggunakan *backup* terhadap jaringan yang mengalami gangguan.
3. Kepala Divisi Teknologi Informasi membuat Lost Event Report serta menginformasikan kronologis dan penanganan yang telah dilakukan kepada Director in Charges.
4. Tindakan pertama setelah penanganan masalah terhadap penyusupan sudah selesai adalah pemberitahuan dari Departemen Keamanan Informasi dan Kontrol Risiko Sistem untuk menerapkan respon/prosedur yang benar.
5. Divisi Teknologi Informasi dengan saran dari Departemen Keamanan Informasi dan Kontrol Risiko Sistem menentukan perubahan yang harus dilakukan untuk mencegah masalah yang sama terulang.
6. Jika diperlukan tindakan hukum, maka bagian terkait termasuk Legal dapat meninjau prosedur untuk mengumpulkan bukti dalam proses hukum dan keterlibatan pihak yang berwenang. Jika pelanggaran itu bersifat internal, tindakannya dapat dilakukan dengan menghubungi Divisi *Human Capital*.

G. *Backup dan Recovery*

1. Melalui persetujuan Manajemen, Divisi Teknologi Informasi menyiapkan sarana backup yang memadai untuk menjamin kelangsungan operasional Bank, sehingga baik sistem bank maupun sistem individu dapat berjalan.
2. Fasilitas *backup* meliputi unit *device* yang dipergunakan maupun sistem operasinya serta jaringan komunikasi.

F. Problem Handling Procedure

1. If a network disruption or communication network attack occurs, the user who first knows of the disruption must immediately notify the Head of the relevant Division / Department / Branch, Head of the Information Technology Division, and the Information Security and System Risk Control Department as soon as possible.
2. Head of the Information Technology Division and the Information Security and System Risk Control Department coordinate to prevent and handle it. For example, cutting off the communication network or using backup on a network that is facing problems.
3. Head of Information Technology Division create Loss Event Report and inform to Director in Charge about the chronological and problem handling.
4. First action after problem is solved, Information Security and System Risk Control Department announce to internal about correct response/procedure.
5. Base on recommendation of Information Security and System Risk Control Department, Information Technology Division determine changes to be done to prevent the same disturbance occurs.
6. If needed, Legal Division refers to procedure, collect evidence for legal process include involve the authority. If internal violation, the action via Human Capital Division.

G. Backup and Recovery

1. By Management approval, Information Technology Division prepare backup to support operational bank and to ensure banking system or individual system continuity.
2. Backup facility includes equipment, operation system (OS) and network communication.

3. Bank dapat menggunakan fasilitas *backup* yang disediakan pihak ketiga (*vendor*), dengan melakukan analisa terlebih dahulu.

3. Bank can use backup facility provided by third party (vendor) by conduct analysis first.

4. Divisi Teknologi Informasi secara rutin melakukan pengujian terhadap perangkat komunikasi maupun fasilitas *backup* lainnya, dalam rangka mengantisipasi kemungkinan terjadinya kegagalan dalam komunikasi. Hasil uji coba yang dilakukan oleh Teknologi Informasi tersebut dilaporkan kepada Departemen Keamanan Informasi dan Kontrol Risiko Sistem dan selanjutnya disampaikan kepada *Director in charge*.

4. Information Technology Division on regular basis testing network device and other backup facility, in order to anticipate communication failure. Testing result is conduct by Information Technology Division, report to Information Security and System Risk Control and submit to Director in charge.

H. Pengujian Berkala Jaringan dan DRP

H. Annual Test of Network and DRP

1. Pengujian terhadap sistem keamanan secara keseluruhan harus dilakukan secara periodik. Uji coba yang dilakukan bukan hanya pada perangkat keamanannya saja, tetapi keseluruhan kebijakan, apakah masih relevan, atau perlu ditingkatkan lagi disesuaikan dengan kondisi terakhir.

1. Network security test is conduct onregular basis. Testing is not only for security equipment but also the policy, whether it is still relevant, or need to be improved according to the last condition.

2. Uji coba jaringan komunikasi *backup* dilakukan minimal 1 (satu) kali dalam setahun sehingga dapat dipastikan bahwa *backup* jaringan tersebut dapat difungsikan sewaktu-waktu. Uji coba yang akan dilakukan harus dikoordinasikan dengan semua pihak yang terkait seperti, pelaksana DRP, dokumentasi, skenario uji coba, dan Izin Direksi untuk melakukan uji coba tersebut.

2. Backup network test conduct at least 1 (once) a year to ensure that network backup can be used at any time. Testing should be coordinate with all related parties such as DRP coordinator, documentation, test scenario and Director approval to conduct test.

3. Setiap uji coba, hasilnya harus dilaporkan ke Direksi secara tertulis yang meliputi, jenis ujicoba (aplikasi, server, line komunikasi yang digunakan untuk uji coba), status terakhir (berhasil/gagal) termasuk perangkat jaringan yang terdapat pada DRC.

3. Testing result is reported to Board of Directors consisting of testing type (application, server, communication line), status (success/fail) include device used in DRC.

4. Menunjuk seorang penanggung jawab (koordinator) yang bertugas untuk membuat skenario pengujian, rencana uji coba, jenis transaksi dan jenis uji coba yang akan dilaksanakan termasuk menunjuk penanggung jawab pada masing- masing Divisi/Departemen/Cabang yang ikut dalam uji coba.

4. Assign a coordinator to make testing scenario, testing plan, transaction type and testing type, include assign PIC at each Division/Department/Branch.

5. Melakukan analisa hasil uji coba, dan memperbaiki/melengkapi kekurangan yang ditemukan dalam ujicoba untuk menjadi perhatian pada uji selanjutnya.

5. Conduct analysis base on testing result and make recommendation for future testing

IV. PENGENDALIAN INTERNAL

A. Audit Internal

Dalam rangka memastikan keamanan jaringan, audit terhadap jaringan komunikasi wajib dilakukan tahunan oleh pihak independen baik Auditor *Intern* maupun Auditor *Ekstern*.

Cakupan audit jaringan antara lain mencakup:

1. Kinerja jaringan komunikasi
2. Akses logik
3. Akses fisik
4. *Remote access*
5. Infrastuktur
6. Dokumentasi

B. Dokumentasi

Dalam melakukan pengendalian jaringan komunikasi, masing-masing Departemen terkait pada Divisi Teknologi Informasi memastikan bahwa dokumentasi terkait jaringan komunikasi lengkap dan terkini yang meliputi:

1. Kebijakan prosedur, standar dan *baseline* mengenai jaringan komunikasi.
2. Diagram jaringan komunikasi.
3. Daftar dan spefisikasi perangkat lunak dan perangkat keras jaringan komunikasi.
4. Daftar permasalahan dan penanganannya.
5. Laporan pemantauan jaringan komunikasi.
6. Laporan perencanaan kapasitas jaringan komunikasi.
7. Kontrak dan SLA dengan pihak ketiga penyedia jasa fasilitas jaringan komunikasi.
8. Dokumen implementasi/perubahan/ pengujian jaringan komunikasi.
9. Daftar *user* dan wewenangnya.
10. Daftar *port* di jaringan internal baik yang digunakan dan yang tidak digunakan.

IV. INTERNAL CONTROL

A. Internal Audit

In order to ensure network security, auditof network communication is mandatory to be done annually by independent party, either Internal Audit or External Audit.

Network audit covering:

1. Network communication performance
2. Logical access
3. Physical access
4. Remote access
5. Infrastructure
6. Documentation

B. Documentation

In control network communication, each Department include Information Technology Division ensure that documentation is comprehensive and up to date include

1. Policy, procedure, standard, and baseline about network communication.
2. Network communication design
3. List and software specification and hardware network communication
4. Problem handling list.
5. Report of network communication monitoring.
6. Report of network communication capacity plan.
7. Agreement and SLA with third party.
8. Document of network communication implementation/changes/testing.
9. User access list.
10. Internal port list (use and unused).

V. PENUTUP

Kebijakan ini diterbitkan dalam 2 (dua) bahasa yaitu Bahasa Indonesia dan Bahasa Inggris, dan bilamana terjadi perbedaan penafsiran antara keduanya maka yang akan menjadi acuan adalah Bahasa Indonesia.

Kebijakan mulai berlaku sejak memperoleh persetujuan Presiden Direktur tanggal 2 Februari 2024 dan Dewan Komisaris tanggal 19 Februari 2024 dan mencabut Kebijakan Jaringan Komunikasi Edisi 5, Februari 2022

Kebijakan Jaringan Komunikasi 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.

V. CLOSING

This policy is published in 2 (two) languages, Indonesian and English, and if there are differences in interpretation between the two then the reference is Indonesian.

This policy is valid since get approval by President Directors on February 2, 2024 and board of Commissioners on February 19, 2024 and revoke Network Communication Policy 5th Edition, February 2022

This policy will be reviewed periodically at least every two years, if necessary as an improvement efforts in accordance with the Bank's business development and the needs of the underlying regulator or company.