Bank Resona Perdania

KEBIJAKAN PENGENDALIAN PUSAT DATA

DATA CENTER MANAGEMENT POLICY

Edisi 7, Juli 2023

7th Edition, July 2023

BOD Approval No. 263/ITD/IT-PLN/X/2023

BOC Approval No. 156/BOC/X/2023-ITD/IT-PLN

DAFTAR ISI

Table of Content

Hal/*Page*

Bab I	**PENDAHULUAN**	**1**	**Chapter I**	**INTRODUCTION**
A.	Latar Belakang	**1**	A.	Background
B.	Acuan	**1-2**	B.	Reference
C.	Tujuan	**3**	C.	Purpose
D.	Ruang Lingkup	**3-4**	D.	Scope
Bab II	**TUGAS DAN TANGGUNG JAWAB**	**5**	**Chapter II**	**JOB AND RESPONSIBILITY**
A.	Direksi	**5**	A.	Direksi
B.	Dewan Komisaris	**5-6**	B.	Board Of Comissioners
C.	Divisi Teknologi Informasi	**6-8**	C.	Information Technology Division
D.	Departemen Keamanan Informasi dan Risiko Sistem	**8**	D.	Information Security and System Risk Department
E.	Divisi Internal Audit	**9**	E.	Internal Audit Division
Bab III	**PROSEDUR PUSAT DATA**	**10**	**Chapter III**	**DATA CENTER PROCEDURE**
A.	Prosedur Pengamanan Pusat Data	**10-11**	A.	Procedure of Data Center Security
B.	Prosedur Akses Pusat Data	**11-12**	B.	Procedure of Data Center Access
Bab IV	**PENUTUP**	**13**	**Chapter IV**	**CLOSING**

I. PENDAHULUAN

A. Latar Belakang

Kebutuhan pengendalian yang memadai atas operasional Pusat Data (*Data Center*) yang memadai atas operasional Pusat Data untuk memastikan pengamanan informasi dilaksanakan secara efektif agar informasi yang dikelola terjaga kerahasiaan, integritas dan ketersediaannya secara efektif dan efisien dengan memperhatikan keputusan terhadap ketentuan yang berlaku.

B. Acuan

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

   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 Pengembangan dan Penguatan Sektor Keuangan;

2. UU RI No.11 Tahun 2008 sebagaimana telah diubah dengan UU RI No.19 Tahun 2016 tentang Informasi dan Transaksi Elektronik;
3. UU RI No.27 Tahun 2022 tentang Pelindungan Data Pribadi;
4. Peraturan Pemerintah Republik Indonesia No.71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
5. Peraturan Menteri Komunikasi dan Informatika Republika Indonesia No.20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik;
6. PBI No. 3 Tahun 2023 tentang Pelindungan Konsumen Bank Indonesia;
7. POJK No.6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat

I. INTRODUCTION

A. Background

The need for adequate control over the operation of the Data Center to ensure that information security is implemented effectively so that the information managed is kept confidential, integrity and availability effectively and efficiently taking into account the decisions against the applicable provisions.

B. Reference

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

   Articles 40 and 41 were revoked by PERPU No. 1 of 2017 on Access to Financial Information for Tax Purposes;

   Some articles were revoked by UU RI No.4 of 2023 on the Development and Strengthening of the Financial Sector.

2. Law of the Republic of Indonesia No. 11 of 2008 as amended by the Law of the Republic of Indonesia No. 19 of 2016 on Electronic Information and Transactions;
3. Law of the Republic of Indonesia No. 27 of 2022 on the Protection of Personal Data;
4. Government Regulation of the Republic of Indonesia No.71 of 2019 on Electronic System Maintenance and Transactions;
5. Regulation of the Minister of Communication and Information of the Republic of Indonesia No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems;
6. PBI No. 3 of 2023 concerning Consumer Protection of Bank Indonesia;
7. POJK No.6/POJK.07/2022 on Consumer and Society Protection in the Financial

di Sektor Jasa Keuangan

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

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

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

10. 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.

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

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

13. Kebijakan Manajemen Risiko secara Umum (Individual);

14. Kebijakan Manajemen Risiko Teknologi Informasi;

15. Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem dalam Penggunaan Teknologi Informasi

16. Kebijakan Tingkat Otorisasi

17. Kebijakan Tugas & Wewenang

18. Kebijakan Job Description

Services Sector

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

9. SEOJK No.21/POJK.03/2017 dated June 6, 2017 on the Application of Risk Management in the Use of Information Technology by Public Banks;

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

10. POJK No.18/POJK.03/2016 on the Application of Risk Management to General Banks;

    Since October 30, 2021, Articles 20, Articles 21, Articles 22, and Articles 24 of POJC No. 18/PoJK.03/2016 concerning the application of risk management to general banks are declared revoked and not in force by POJQ No.13/POYK.03/2021 on the Maintenance of General Bank Products.

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

12. SEOJK No.29/SEOJK.03/2022 dated December 27, 2022 on Cyber Resilience and Security for Public Banks.

13. General Individual Risk Management Policy (individual);

14. Risk Management Policy of Information Technology;

15. Information Security and System Risk Management Policy in the use of Information Technology;

16. Authorization Level Policy

17. Duties & Authorities Policy

18. Job Description Policy

C. Tujuan

Sebagai peraturan dasar kegiatan operasional Pusat Data dalam menjaga dan mengamankan sistem, data dan jaringan komunikasi kritikal Bank Resona Perdania (“Bank”), baik yang berada di lokasi Pihak Ketiga dan di lokasi Kantor Pusat Bank.

C. Purpose

Basic rule of Data Center operation activity in order to maintain and secure the critical system, data and network of Bank Resona Perdania (“Bank”), that located both in Third Party and in Bank Head Office.

D. Ruang Lingkup

1. Definisi

Pusat Data adalah fasilitas utama pemrosesan data Bank yang terdiri dari perangkat keras dan sistem. Pusat Data yang diatur dalam Kebijakan ini adalah ruang Pusat Data yang berada di lokasi Pihak Ketiga dan yang berada di Kantor Pusat Bank. Penyedia jasa Pusat Data yang diatur dalam Kebijakan ini adalah pihak ketiga yang menyediakan sarana dan prasarana sehingga Bank dapat menyelenggarakan kegiatan operasional Pusat Data.

2. Ketersediaan

Pusat Data dijaga untuk mendukung kegiatan operasional Bank secara berkesinambungan.

3. Pengamanan

Pengamanan Pusat Data dirancang sedemikian mungkin untuk mendukung kegiatan operasional rutin maupun non-rutin, yang dapat dimonitor secara fisik maupun non-fisik.

4. Kebijakan

Sistem dan prosedur serta standar yang diterapkan dalam aktifitas operasional Pusat Data mencakup aktivitas menjalankan tugas rutin maupun nonrutin. Aktivitas yang terkait dengan operasional Pusat Data antara lain :

4.1 Penjadwalan Tugas

Bank wajib memiliki dan melaksanakan jadwal semua tugas yang harus dijalankan di Pusat Data Operasional TI efektif dan aman dari perubahan yang tidak sah.

D. Scope

1. Definition

The data center is the main facility for the processing of the bank's data, consisting of hardware and systems. The data center defined in this policy is a data center space located at a third-party location and located at the central office of a bank. Data center service providers defined by this policy are third parties that provide the means and facilities so that the bank can organize the operational activities of the data center.

2. Availability

The data center isined to support the Bank's operational activities continuously.

3. Security

Data Center security is designed as much as possible to support both routine and non-rutine operational activities, which can be monitored physically as well as non-physically.

4. Policy

Systems and procedures and standards are applied in the operational activities of the Data Center includes stints activity routine and nonroutine. Activities related to the operation of the Data Center include:

4.1 Scheduling Tasks

Banks are required to have and implement a schedule of all tasks to be executed in the Data Center IT Operations effective and safe from unauthorized changes.

4.2 Pengoperasian tugas :

Pemberian akses *command line* kepada operator TI harus dibatasi sesuai kewenangan pada fungsi pengoperasian tugas yang telah ditentukan.

4.3 Pendistribusian Laporan/*output* :

Hasil informasi yang diproduksi oleh sistem (*output*), dalam bentuk *softcopy* atau *hardcopy*, dapat merupakan informasi yang sensitif atau rahasia. Prosedur yang harus dimiliki Bank meliputi penentuan informasi yang akan diproduksi, pendistribusian *output* baik secara fisik maupun logik dan pemusnahan *output* yang sudah tidak diperlukan lagi. Prosedur tersebut diperlukan untuk menghindari terbukanya informasi yang bersifat rahasia dan meningkatnya biaya akibat adanya *output* yang tidak diperlukan, dan untuk dapat memastikan keamanan *output*.

4.4 Proses *backup* baik *on-site* maupun *off-site*, *restore*, *download* dan *upload* untuk data/*database*.

4.5 Pengaktifan jejak audit (*audit trail*)

4.2 The operation tasks:

Granting access to the command line IT operators must be restricted within their authority on the functioning of the operation of the task that has been determined.

4.3 Distribution Report / output:

The results produced by the system information (output), in the form of softcopy or hardcopy, can be a sensitive or confidential information. The procedure to be held by the Bank includes determining the information to be produced, the distribution of output both physically and logically and extermination outputs that are not needed anymore. The procedure is necessary to avoid exposure of confidential information and increased costs due to output are not needed, and to be able to ensure the safety output.

4.4 The process of both onsite and offsite backup, restore, download and upload of data / database.

4.5 The activation of the audit trail (audit trail)

II. TUGAS DAN TANGGUNG JAWAB

A. Direksi

1. Memastikan tersedianya sumber daya manusia (SDM) yang cukup dan kompeten sesuai dengan kebutuhan.

2. Memastikan terdapat upaya peningkatan kompetensi SDM terkait penyelenggaraan TI diantaranya melalui pendidikan atau pelatihan yang memadai dan program edukasi untuk meningkatkan kesadaran atas pengamanan informasi.

3. Memastikan struktur organisasi manajemen proyek dari seluruh proyek terkait TI digunakan dengan maksimal dan

4. Memastikan bahwa Bank memiliki kontrak tertulis yang mengatur peran, hubungan, kewajiban, dan tanggung jawab dari semua pihak yang terikat kontrak tersebut, serta memiliki keyakinan bahwa kontrak tersebut merupakan perjanjian yang berkekuatan hukum dan melindungi kepentingan Bank, dalam hal Bank menggunakan jasa pihak lain.

B. Dewan Komisaris

1. Mengevaluasi, mengarahkan, dan memantau kebijakan manajemen risiko di bidang TI dan kesesuaian penerapannya dengan karakteristik, kompleksitas, dan profil risiko Bank.

2. Memberikan arahan perbaikan atas pelaksanaan kebijakan manajemen risiko di bidang TI.

II. JOB AND RESPONSIBILITY

A. Director

1. Ensure the availability of sufficient and competent human resources (HR) according to needs.

2. Ensuring that there are efforts to improve HR competencies related to IT implementation, including through adequate education or training and educational programs to increase awareness of information security.

3. Ensure that the project management organization structure of all IT related projects is used to the maximum and

4. Ensure that the Bank has a written contract that regulates the roles, relationships, obligations and responsibilities of all parties bound by the contract, and has confidence that the contract is a legal agreement and protects the interests of the Bank, in the event that the Bank uses the services of other parties.

B. Board of Commissioners

1. Evaluate, direct, and monitor risk management policies in the IT field and suit their application with the characteristics, complexity, and risk profile of the Bank.

2. Provide direction for improvement on the implementation of riskvmanagement policies in the IT field.

3. Melakukan evaluasi terhadap perencanaan dan pelaksanaan audit, memastikan audit dilaksanakan dengan frekuensi dan lingkup yang memadai, serta melakukan pemantauan atas tindak lanjut hasil audit yang terkait dengan sistem informasi, dan

3. Evaluate the planning and implementation of audits, ensure that audits are carried out with adequate frequency and scope, and monitor the follow-up of audit results related to the information system, and

4. Melakukan evaluasi terhadap pengelolaan pengamanan yang andal dan efektif atas TI guna menjamin ketersediaan,kerahasiaan, dan keakuratan informasi.

4. Evaluate reliable and effective security management of IT to ensure availability, confidentiality and accuracy of information.

C. Divisi Teknologi Informasi

C. Information Technology Division

1. Bertanggung jawab melakukan pemeriksaan berkala terkait peralatan, sistem dan data di Pusat Data dan melaporkan kepada *Director in Charge* dan Kepala Divisi Teknologi Informasi ketika terjadi masalah.

1. Responsible to check on regular basis the equipment, system and data in Data Center, also to report to Director in Charge and Head of Information Technology Division in case problem occurs.

2. Bertanggung jawab atas keamanan akses ke ruang Pusat Data dan menjaga agar rak dalam keadaan tertutup.

2. Responsible of access into Data Center and always keep rack in close condition;

3. Bertanggung jawab dalam melakukan inventaris perangkat keras dan peralatan ruang Pusat Data secara berkala.

3. Responsible to perform a regular basis inventory of hardware and equipment in Data Center.

4. Bertanggung jawab untuk melakukan pemeriksaan Pusat Data secara rutin dan mendokumentasikannya.

4. Responsible to perform regular basis checking, also maintain the documentation;

5. Bertanggung jawab untuk memonitor kapasitas penggunaan *UPS* di Kantor Pusat.

5. Responsible to monitor UPS usage capacity in Head Office.

6. Melakukan administrasi terhadap User/Vendor

6. Administrative of User/Vendor who will enter Data Center room.

7. 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:

7. Reporting obligations with reference to incidental reporting provisions as listed in section 60 of POJK No.11/POJK.03/2022 on Information Technology Maintenance by the General Bank are:

    1. In case of information technology (IT) incidents that are potentially and/or have caused significant losses and/or interfere with the smooth operation of the bank, the bank shall provide:

        a. Initial notification no later than 24

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 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.

5. 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.

8. 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 :

a. Bank wajib menyampaikan laporan berkala dan laporan insidental.

b. Laporan insidental dimaksud antara lain terdiri atas laporan gangguan dalam pemrosesan transaksi pembayaran dan tindak lanjut yang

hours after the IT incident is known; and

b. IT incident report no later than 5 working days after the general IT incident has been known.

2. Preliminary notification pursuant to paragraph (1a) is submitted by electronic means in writing to the OJK on the basis of the initial information available.

3. IT incident reports, according to paragraphe (1b), are part of the report of the condition that is potentially causing significant loss to the bank's financial condition in accordance with the POJC regarding the implementation of risk management for the bank;

4. In the event that there are other authority arrangements concerning the submission of the initial notification and/or IT incident report within a period of time earlier than the time period in accordance with paragraph (1), the Bank shall submit the initial notification and / or report of the IT incident to the OJK at the same time according to the provisions of the legislation of the other authorities concerned.

5. Bank which has submitted an initial notification and/or report of an IT incident in accordance with paragraph (4) shall be deemed to have complied with the requirements of paragraph (1) letter a and/ or letter b.

8. When there is an interruption in the processing of payment transactions to refer to the provisions as listed in the BI Letter No. 25/254/DSSK/Srt/Rhs dated 20June 2023 concerning the Incidental Reporting Obligation. The incidental report can be submitted through the designated PIC. In PBI No. 14/23/PBI/2012 dated December 26, 2012 on Transfer of Funds (PBI TD) Banks are obliged to submit the following things:

a. Banks shall submit periodic reports and incidental reports.

b. Incidental reports shall consist, inter alia, of reports of interruption in the processing of payment transactions and follow-up that have been carried out,

telah dilakukan, dan laporan terjadinya keadaan kahar (force majeure) atas penyelenggaraan pemrosesan transaksi pembayaran.

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

d. Penyampaian laporan gangguan wajib disampaikan paling lambat 3 hari setelah kejadian, dan laporan keadaan kahar wajib disampaikan paling lambat 3 hari kerja setelah kejadian.

and reports of occurrence of force majeure on the maintenance of processing payment transaction.

c. The occurrence and occurence of force major shall be notified to Bank Indonesia no later than 1 (one) hour after the event.

d. The submission of the report of interference shall be submitted not later than 3 days after the occurrence, and the obligatory report of the circumstances of the event shall be presented no later as 3 working days after that event.

9. Kewajiban laporan rencana penggunaan pihak penyedia jasa dalam penyelenggaraan Pusat Data (Data Center), Disaster Recovery Center dan/atau Pemprosesan Transaksi Berbasis Teknologi di dalam negeri paling lambat 2 (dua) bulan sebelum kegiatan tersebut efektif dioperasikan.

9. Liability report the planned use of service providers in the implementation of Data Center (Data Center), Disaster Recovery Center and / or Transaction Processing Technology Based in the country no later than two (2) months prior to the effective operation of these activities.

10. Laporan realisasi rencana penyelenggaraan Pusat Data (Data Center), Disaster Recovery Center dan/atau Pemprosesan Transaksi berbasis teknologi oleh pihak penyedia jasa paling lambat 1 (satu) bulan sejak kegiatan tersebut efektif dioperasikan.

10. Report on the realization of plans for the implementation of Data Centers, Disaster Recovery Centers and/or technology-based Transaction Processing by service providers no later than 1 (one) month after the activities are effectively operated.

D. Departemen Keamanan Informasi dan Risiko Sistem

1. Melakukan evaluasi terhadap Pusat Data termasuk kemungkinan gangguan pada peralatan, sistem dan data di Pusat Data.

2. Melakukan monitor dan kajian terhadap log aktifitas pengunjung Pusat Data.

3. Melakukan kajian akses ke ruang Pusat Data secara berkala berdasarkan tugas dan tanggung jawab.

4. Memberikan rekomendasi berdasarkan kajian dan analisis yang dilakukan untuk meningkatkan keamanan Pusat Data.

D. Information Security and System Risk Department

1. Perform evaluation about Data Center include problem in the equipment, system and data in Data Center.

2. Monitor and review activity log of Data Center visitor.

3. Perform review on regular basis the Data Center access based on job and responsibility.

4. Submit recommendation based on review and analysis result in order to improve Data Center security

E. Divisi Internal Audit

Divisi Internal Audit wajib menyampaikan hasil audit Teknologi Informasi yang dilakukan pihak independen terhadap Pusat Data (*Data Center*) dan/atau *Disaster Recovery Center* dan/atau Pemrosesan Transaksi Berbasis Teknologi yang penyelenggaraannya dilakukan oleh pihak penyedia jasa kepada Otoritas jasa Keuangan paling lambat 2 (dua) bulan setelah audit selesai dilakukan

E. Internal Audit Division

Internal Audit Division must submit the results of the audit of Information Technology conducted an independent party to the Data Center (Data Center) and / or Disaster Recovery Center and / or Processing Transaction-based technology implementation is done by the service provider to the Authority Financial services no later than 2 (two) months after the audit is completed.

III. PROSEDUR PUSAT DATA

A. Prosedur Pengamanan Pusat Data

1. Pengendalian Akses Fisik Pusat Data

1.1. Pintu atau akses ke ruang Pusat Data Bank harus terkunci dan dilengkapi dengan sistem yang dapat mengatur atau monitor akses.

1.2. Ruang Pusat Data dirancang sedemikian mungkin untuk mencegah pihak yang tidak berhak masuk atau memonitor ruang Pusat Data Bank.

1.3. Bank memiliki dan memelihara logbook untuk mencatat setiap akses ke ruang Pusat Data.

1.4. Setiap perubahan pada Sistem yang berada dalam ruang Pusat Data didokumentasikan dan harus berdasarkan checklist yang ditandatangani oleh pihak terkait.

2. Pengendalian Lingkungan Pusat Data

2.1 Memastikan bahwa ruang Pusat Data memiliki suhu dan kelembaban yang sesuai dengan melakukan pemeriksaan secara berkala;

2.2 Memastikan kecukupan sumber listrik yang stabil.

2.3 Mengantisipasi ketidakcukupan sumber listrik dengan menggunakan UPS.

2.4 Memastikan ruang Pusat Data memiliki alat pendeteksi asap dan api yang dapat beroperasi secara otomatis ataupun manual.

2.5 Menggunakan raised floor untuk pengamanan kabel dan menghindari efek grounding.

2.6 Di dalam ruangan Pusat Data tidak diperkenankan untuk makan, minum dan/atau merokok.

III. DATA CENTER PROCEDURE

A. Procedure of Data Center Security

1. Controlling Physical Access of Data Center

1.1. Door or access into Bank Data Center should always be locked and equipped with system to manage or monitor access.

1.2. Data Center room is designed to prevent unauthorized party to enter or monitor Bank Data Center.

1.3. Bank has and maintain logbook to record every access into Data Center room.

1.4. Every system change in Data Center must base on checklist that made by respective party and must be signed by authorized party before filing.

2. Controlling Environment of Data Center

2.1 Perform a regular base checking of Data Center temperature and humidity.

2.2 Ensure the adequacy and stability of electric power.

2.3 Anticipate the inadequacy of electric power by using the UPS.

2.4 Ensure the operation of smoke detector and fireextinguisher can be in both automatic and manual.

2.5 Use raised floor to secure cable and prevent grounding effect;

2.6 In Data Center is prohibited to eat, drink and/or smoking.

2.7 Setiap penambahan dan/atau perubahan sistem yang berada dalam ruang Pusat Data harus didokumentasikan, atas se-pengetahuan dan telah mendapatkan ijin dari Director in Charge dan/atau Kepala Divisi Teknologi Informasi atau Kepala Departemen perencanaan TI dan Fungsi Operasional dan Dukungan TI.

Pemeriksaan terhadap peralatan dalam ruang Pusat Data Bank dilakukan setiap hari untuk memastikan kelangsungan operasional Pusat Data.

B. Prosedur Akses Pusat Data

1. Ruang Pusat Data hanya dapat diakses oleh personil Divisi Teknologi Informasi. Selain dari itu harus didampingi oleh personil Divisi Teknologi Informasi;

2. Prosedur akses ke dalam ruang Pusat Data yang berada di dalam lokasi Pihak Ketiga menggunakan prosedur yang berlaku di Pihak Ketiga tersebut.

3. Setiap User/Vendor selain Departemen perencanaan TI dan Fungsi Operasional dan Dukungan TI yang akan memasuki ruangan Pusat Data harus menyerahkan data identitas untuk dibuatkan surat izin masuk oleh Divisi Teknologi Informasi.

4. User yang sudah dibuatkan surat izin masuk oleh Divisi Teknologi Informasi selanjutnya akan dikirimkan melalui email oleh PIC yang *authorize* di Pusat Data, yang akan ditujukan ke *email* pihak ketiga penyedia Pusat Data, agar bisa diberikan izin masuk ruang Pusat Data.

5. Setiap *email* yang diterima pihak ketiga penyedia Pusat Data, akan di proses dan mengkonfirmasi ulang melalui *email*.

6. Setiap orang yang masuk ke dalam ruang Pusat Data mengisi *logbook* dan menuliskan tujuannya.

7. Akses ke ruang Pusat Data di luar jam kerja harus melalui persetujuan Director in Charge dan Kepala Divisi Teknologi

2.7 Every addition and/or system change in Data Center room is documented, must by acknowledge and approval of Director in Charge and/or Head of Information Technology Division or Head of IT Planning Department and IT Operations and Support Function

Regular base equipment checking in Bank Data Center is performed daily to ensure the continuity of Data Center operation.

B. Procedure of Data Center Access

1. Data Center room can only be accessed by Information Technology Division personnel. Other than that must be accompanied by Information Technology Division personnel.

2. Procedure access into Data Center room that located in Third Party is following the procedure of the respective party.

3. Every User/Vendor other than IT Planning Department and IT Operations and Support Function who will enter Data Center room must submit identity data to create visit form request by Information Technology Division.

4. Users who already made entry permits by the Division of Information Technology will then be sent via email by the PIC which authorize in the data center, which will be directed to a third-party email data providers, in order to be granted permission to enter the room Data Center

5. Any Emails received third-party data center providers, will be processed and re-confirm by email.

6. Every person who access into Data Center room must register in logbook and write its purpose.

7. Access into Data Center on non-working hour must get approval of Director in Charge and Head of

Informasi.

8. Akses ke ruang Pusat Data pada hari libur melalui prosedur yang berlaku di Bank.

9. Sebagai usaha pengamanan informasi, setiap personil dan/atau Pihak Ketiga yang melakukan aktivitas di dalam ruang Pusat Data tidak diperbolehkan untuk mengambil gambar tanpa persetujuan Kepala Divisi Teknologi Informasi.

10. Jika aktivitas di atas telah disetujui, maka harus didampingi oleh personil Departemen perencanaan TI atau Fungsi Operasional dan Dukungan TI.

Information Technology Division.

8. Access into Data Center on non working day must follow Bank procedure.

9. As an effort of information security, every activity of personnel and/or Third Party in Data Center room is prohibited to take any picture/information without approval from Head of Information Technology Division.

10. If the above activities have been approved, they must be accompanied by IT planning Department personnel or IT Operations and Support Functions

IV. PENUTUP

Kebijakan Pengendalian Pusat Data 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 Pengendalian Pusat Data ini mulai berlaku sejak memperoleh persetujuan Presiden Direktur tanggal 16 Oktober 2023 dan Dewan Komisaris pada tanggal 23 Oktober 2023 dan mencabut Kebijakan Pengendalian Pusat Data Edisi 6, Januari 2022.

Kebijakan Pengendalian Pusat Data 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.

IV. CLOSING

Data Center Control Policy is published in 2 (two) languages, Bahasa and English, and if there are differences in interpretation between the two then the reference is Bahasa.

Data Center Control Policy valid since approval of the President Director on October 16, 2023 and Board of Commissioners on October 23, 2023 and revoke the Data Center Control Policy 6th Edition, January 2022.

Data Center Control Policy will be reviewed regularly at the latest every 2 (two) years or if needed as an improvement effort in accordance with the business development and needs of the Bank or changes in the underlying regulations.