Bank Resona Perdania

PEDOMAN INTERNET DAN EMAIL
INTERNET AND EMAIL GUIDELINE

Edisi 4, April 2023

4th Edition, April 2023

BOD Approval No.144/ITD/IT-PLN/VI/2023

DAFTAR ISI
Table of Content

Hal/*Page*

Bank Resona Perdania

I. PENDAHULUAN

A. Latar Belakang

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

B. Acuan

1. Undang - Undang Republik Indonesia No. 11 Tahun 2008 sebagaimana telah diubah dengan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik;

2. Peraturan Menteri Komunikasi dan Informatika RI No.20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

3. Peraturan Menteri Komunikasi dan Informatika RI No.5 Tahun 2020 sebagaimana telah diubah dengan Peraturan Menteri Komunikasi dan Informatika No. 10 Tahun 2021 tentang Penyelenggara Sistem Elektronik Lingkup Privat.

4. Peraturan Menteri Komunikasi dan Informatika No.11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik

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

6. 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

7. 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

I. PRELIMINARY

A. Background

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

B. Reference

1. Regulation of the Republic of Indonesia No.11 of 2008 as amended by Regulation No.19 of 2016 about Information and Electronic Transaction;

2. 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.

3. Regulation of the Minister of Communication and Informatics of the Republic of Indonesia No.5 of 2020 as amended by Regulation of the Minister of Communication and Informatics No. 10 of 2021 concerning Private Electronic System Operators.

4. Regulation of the Minister of Communication and Informatics No.11 of 2022 concerning the Governance of Electronic Certification

5. POJK No.11/POJK.03/2022 concerning Application of Information Technology by Commercial Banks;

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

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

7. POJK No.18/POJK.03/2016 about The Application of Risk Management for Commercial Banks.

   Since October 30, 2021, Article 20, Article 21, Article 22 and Article 24 in POJK No.

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

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.

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

8. SEOJK No. 34/SEOJK.03/2016 dated 1 September 2016 about Risk Management Implementation for Commercial Bank;

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

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

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

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

11. POJK N0.6/POJK.07/2022 tentang Perlindungan Data Konsumen dan Masyarakat di Sektor Jasa Keuangan

11. POJK No.6/POJK.07/2022 concerning Protection of Consumer and Public Data in the Financial Services Sector.

    a. semua peraturan pelaksana dari POJK No.1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan; dan

    a. all implementing regulations of POJK No.1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector; and

    b. ketentuan-ketentuan pelaksana yang mengatur Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan,

    b. implementing provisions governing Consumer and Public Protection in the Financial Services Sector,

dinyatakan tetap berlaku sepanjang tidak bertentangan dengan POJK ini.

declared to remain valid as long as it does not conflict with this POJK.

    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;

    c. POJK No.1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector and implementing provisions regarding data confidentiality and data security and/or consumer personal information;

    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

    d. Article 32 POJK No.76/POJK.07/2016 concerning Increasing Financial Literacy and Inclusion in the Financial Services Sector for Consumers and/or the Public; And

    e. PBI No.7/6/PBI/2005 tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah,

    e. PBI No.7/6/PBI/2005 concerning Information Disclosure of Bank Products and Use of Customer Personal Data,

dicabut dan dinyatakan tidak berlaku

revoked and declared no longer valid

12. 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

13. Keputusan Bersama Menteri Komunikasi dan Informatika RI, Jaksa Agung RI, dan Kepala Kepolisian Negara RI No.229 Tahun 2021, No.154 Tahun 2021, No.KB/2/VI/2021 tentang Pedoman Implementasi Atas Pasal Tertentu Dalam UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan UU No.19 Tahun 2016 tentang Perubahan atas UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

14. Kebijakan Tingkat Otorisasi

15. Kebijakan Komite Pengarah Teknologi Informasi;

16. Kebijakan Manajemen Risiko Umum (Individual);

17. Kebijakan Manajemen Risiko Teknologi Informasi;

18. Kebijakan Pengawasan Keamanan Sistem dan Informasi;

19. Kebijakan Pengelolaan Situs Web;

20. Kebijakan Pengamanan Informasi dan Manajemen Risiko Sistem dalam Penggunaan Teknologi Informasi;

21. Kebijakan Anti Virus;

22. Kebijakan Tugas & Wewenang;

23. Kebijakan Uraian Pekerjaan;

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

    Implementation provisions governing Consumer and Community 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

13. Joint Decree of the Minister of Communication and Information of the Republic of Indonesia , the Attorney General of the Republic of Indonesia, and the Chief of Police Number 229 of 2021, Number 154 of 2021, Number KB/2/VI/2021 concerning Guidelines for the Implementation of Certain Articles in Law No. 11 of 2008 concerning Information and Electronic Transactions as amended by Law no. 19 of 2016 concerning Amendments to Law no. 11 of 2008 concerning Information and Electronic Transactions.

14. Levelling of Authority Policy;

15. Information Technology Steering Committee Policy;

16. General Risk Management Policy (Individual);

17. Information Technology Risk Management Policy;

18. System and Information Security Monitoring Policy;

19. Website Management Policy;

20. Information Security and System Risk Management in the Use of Information Technology Policy;

21. Anti Virus Policy;

22. Duties & Authorities Policy;

23. Job Description Policy;

C. Tujuan

1. Memastikan pemeliharaan integritas internet dan *email*.
2. Memaksimalkan kinerja internet dan *email*.
3. Memastikan pengelolaan, penggunaan, pengawasan / kontrol, keamanan internet dan *email* dilakukan secara maksimal.
4. Meminimalkan kemungkinan risiko terkait penggunaan internet dan *email*.

D. Ruang Lingkup

1. Keamanan

   Internet dan *email* harus dirancang, dikonfigurasi dan mempunyai tingkat kontrol yang tinggi untuk melindungi Bank dari risiko yang mungkin terjadi (internal dan/atau eksternal).

2. Ketersediaan

   Bank harus meyakini bahwa jaringan internet dan *email* dapat dipergunakan setiap saat. Jika terdapat keadaan darurat, dalam hal ini mengalami gangguan internet atau *email*, Bank harus segera menghubungi pihak ketiga agar gangguan tersebut dapat segera terselesaikan.

3. Kerahasiaan

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

4. Penggunaan

   Segala penggunaan internet dan *email* di lingkungan internal Bank diatur dalam prosedur-prosedur untuk meminimalkan kemungkinan risiko terkait internet dan *email*.

5. Penanganan Masalah

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

C. Purpose

1. Ensure maintenance of internet and email integrity.
2. Maximize network performance.
3. Ensure a maximal internet and email maintenance, usage, control and security.
4. Minimize risk of internet and emal usage.

D. Scope

1. Security

   Internet and email is designed, configured and highly controlled in order to protect Bank from potential risk (internal and/or external).

2. Availability

   Bank has to make sure internet and email availability. During emergency, in this case disruption internet or email, Bank should immediately contact Vendor / third party so that disruption can be immediately resolved.

3. Confidentiality

   To prevent risk related to internet and email, network configuration and access should be limited to authorized and/or authorized vendor.

4. Usage

   To minimize internet and email risk, all intenet and email usage is determined in procedures.

5. Problem Handling

   All problem handling should refer to procedure and should be documented in order to improve problem handling.

II. PERAN DAN TANGGUNG JAWAB

A. Direksi

1. Memastikan adanya pengawasan yang memadai terkait penggunaan internet dan *email*.
2. Mempertimbangkan kebutuhan jaringan yang sesuai dengan kondisi bisnis dan strategi yang akan dikembangkan.
3. Memberikan persetujuan jika jaringan yang digunakan oleh sistem yang terkait Regulator dan/atau Nasabah Bank akan terkoneksi dengan pihak ketiga, berdasarkan analisa dan diskusi dengan Komite Pengarah TI.
4. Menetapkan prosedur dan kebijakan terkait internet dan *email* agar kontrol terhadap internet dan *email* dapat dilakukan dengan baik, efisien dan keamanan terjamin.
5. Menunjuk administrator (Divisi Teknologi Informasi / Departemen Perencanaan TI dan Fungsi Operasional & Dukungan Teknologi) yang berkualifikasi untuk bertanggung jawab terhadap pengembangan jaringan, ketersediaan, keamanan dan kebutuhan jaringan dan berkoordinasi dengan Departemen Pengawas Keamanan Informasi dan Kontrol Risiko Sistem.

B. Divisi Teknologi Informasi / Departemen Perencanaan TI dan Fungsi Operasional & Dukungan Teknologi

1. Bertanggung jawab terhadap pemberian akses internet atau *email* kepada *user* yang berkepentingan.
2. Memblokir situs-situs terlarang yang tidak berkaitan dengan pekerjaan.

II. JOB AND RESPONSIBILITY

A. Board of Director

1. Ensure an adequate internet and email usage monitoring.
2. Considering network requirement align with business condition and business plan.
3. Giving approval if network used by system related to regulators and / or customer bank that will be connected with third party, which based on analysis and IT Steering Committee.
4. Approve internet and email procedure and policy to ensure internet and email control is good, efficient and secured.
5. Assign administrator (Information Technology Division / Information Technology Planning Department and Operational Function & IT Support) that qualified and responsible to network development, availability, security and network requirement and coordinate with Information Security and System Risk Controller Department.

B. Information Technology Division / Information Technology Planning Department and Operational Function & IT Support

1. Responsible for giving an access internet or email for related users.
2. Blocking illegal sites that unrelated to the job.

3. Mengelola sistem *filtering* setiap aktifitas *email* yang masuk maupun keluar.

4. Dalam hal mekanisme aktifitas proses *blocking* situs internet Divisi Teknologi Informasi juga menerima laporan dari *user* dan Departemen Pengawas Keamanan Informasi dan Kontrol Risiko Sistem terkait situs – situs yang tidak berkaitan dengan pekerjaan untuk diblokir.

C. Departemen Pengawas Keamanan Informasi dan Kontrol Risiko Sistem

1. Memastikan bahwa Pedoman internet dan *email* sudah diimplementasikan dan dilaksanakan sesuai dengan ketentuan.

2. Melakukan pengawasan, pemantauan, peninjauan dan memberikan rekomendasi kepada Divisi TI mengenai efektifitas penggunaan internet dan *email* berdasarkan data dan laporan dari Divisi TI.

3. Melakukan pemeriksaan dan *monitoring* secara berkala terhadap pengaturan parameter, *log* dan/atau audit *trail* pada aktifitas penggunaan internet dan *email*.

4. Melakukan identifikasi / investigasi terhadap masalah / *problem* / kelemahan yang terjadi pada jaringan, baik internal maupun eksternal yang berkaitan dengan keamanan dan kebijakan.

5. Melakukan kontrol aktifitas internet dan *email* yang dilakukan oleh user dan pengawasan terhadap pengiriman *email* keluar harus menggunakan *password* untuk *file attachment*.

D. Pengguna

1. Dilarang menggunakan/mengakses situs-situs yang berhubungan dengan konten pornografi, SARA, video streaming.

2. Bertanggung jawab dalam menggunakan jaringan, baik dalam menggunakan internet, *email*, serta jaringan yang digunakan untuk lalu lintas data, dan lain-lain.

3. Dilarang menggunakan *email* kantor untuk keperluan pribadi yang tidak berhubungan

3. Manage filtering system every incoming and outgoing email activity.

4. The mechanism of internet sites blocking activity , IT Division receive report from user and Information Security and System Risk Controller Department for blocking the sites that unrelated to the job.

C. Information Security and System Risk Controller Department

1. Ensure that Internet and Email Guideline is implemented and carried out following the rule.

2. Conduct monitoring, supervision, review and give recommendation to IT Division about internet and email usage effectiveness based on data and report from IT Division.

3. Conduct network access assessment and monitoring on regular basis for parameter control, log and/or audit trail in internet and email usage.

4. Conduct identification/investigation of network problem/weakness, both internal and external that related to security and policy.

5. To control internet and email activity performed by users and oversight of outgoing email should use a password for the file attachment.

D. User

1. Forbidden to use/access to sites that are related to pornographic, racism, video streaming.

2. Responsible in the use of network, internet, email and other network communication.

3. Forbidden to use internal email for personal purpose that are not related to

dengan pekerjaan.

4. Dilarang menggunakan *email* pribadi untuk keperluan kantor, kecuali mendapatkan persetujuan dari Kepala Divisi Teknologi Informasi dan Departemen Pengawas Keamanan Informasi dan Kontrol Risiko Sistem serta diketahui oleh Direktur terkait.

E. Pihak Ketiga

1. Pihak ketiga yang akan menggunakan jaringan Bank dalam rangka perbaikan / perawatan / instalasi / pengujian harus mendapatkan persetujuan terlebih dahulu dari Kepala Divisi Teknologi Informasi.
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.
4. Penggunaan jaringan oleh pihak ketiga harus dilengkapi dengan dokumentasi, berupa *Request Form* media intramart dan laporan hasil pekerjaan.

work.

4. Forbidden to use personal email for office purpose, except approved by Head of Information Technology Division and Information Security and System Risk Controller Department and acknowledge by Director in Charge.

E. Third Party

1. Before using Bank's network for repair / maintenance / installation / testing, third party has to get approval first from Head of Information Technology Division.
2. Network access by third party is limited and is not allowed to access other network, unless is stated otherwise (example for audit purposes).
3. Network access for third party is for temporary and has to close/block after use.
4. Network usage by third party has to support by Intramart media Request Form and working sheet report.

III. ATURAN PENGGUNAAN

A. *Internet*

1. Aturan Mengenai Penggunaan Internet

a. Internet harus dikontrol dan dibatasi hanya untuk keperluan pekerjaan.

b. *Download* harus dilakukan dari situs yang dapat dipercaya untuk menghindari risiko virus dan lain-lain.

c. Informasi yang didapatkan dari internet harus diverifikasi terlebih dahulu sebelum dapat dipergunakan untuk tujuan bisnis perusahaan.

d. Untuk dapat menggunakan internet, *user* harus menyerahkan *User Form* media intramart dan Pernyataan Pendaftar Fasilitas *email* atau Internet. Persetujuan atau penolakan atas penggunaan berdasarkan tingkat kebutuhan pekerjaan.

e. User hendaknya mengetahui bahwa setiap penggunaan aktifitas koneksi terhadap jaringan / internet / *email* direkam dan di*monitor*.

f. Departemen Pengawas Keamanan Informasi dan Kontrol Risiko Sistem melakukan pengawasan dan *review* terhadap akses internet. Penyalahgunaan internet akan diinformasikan kepada *Director in Charge* dan ke atasan terkait juga akan terkena sanksi seperti blokir akses Internet.

g. Dilarang untuk melakukan registrasi terhadap situs/*group* tertentu yang tidak berhubungan dengan kegiatan operasional, terkait kemungkinan risiko *virus* / *worm* / *trojan* dan lain-lain.

h. Dilarang melakukan transaksi *online* melalui fasilitas Internet kantor, kecuali untuk kepentingan pekerjaan.

i. *User* dilarang untuk melakukan koneksi ke internet menggunakan metode koneksi lainnya misalnya *dial-up*, *mobile modem*, nirkabel (*Wi-fi Public*) dan lain-lain, kecuali untuk kepentingan tertentu dan dengan sepengetahuan

III. USAGE GUIDELINE

A. Internet

1. Procedure of Internet Usage

a. Internet is controlled and limited for work only.

b. Download only from trusted sites to prevent virus and other risk.

c. Always verify information from Internet before use it for business purpose.

d. To use Internet, user submit intramart media User Form and Statement For E-mail and Internet Facility Applicant. Approval or reject base on job requirement.

e. User aware that network / internet / email activity is logged and monitored.

f. Information Security and System Risk Controller Department supervise and review Internet access. Internet misuse will be reported to Director in Charge and related Head, include get penalty such as block the Internet access.

g. Prohibited to register into site/group that is not related due to risk of virus / worm / trojan and other.

h. Prohibited to use Internet for online transaction, unless for work related.

i. User is prohibited to connect Internet using other connection method, example dial up, mobile modem, Public Wi-Fi, except for work related and with acknowledge from Head of Information Technology Division and

dan persetujuan Kepala Divisi Teknologi Informasi dan Departemen Pengawas Keamanan Informasi dan Kontrol Risiko Sistem. Dalam hal untuk kepentingan yang berhubungan dengan pekerjaan yang dilakukan di luar kantor maka hal tersebut dikecualikan, mengingat kondisi saat ini dimana perusahaan memberlakukan kerja *shift* WFH dan WFO.

Information Security and System Risk Controller Department. Except for the things that related of work which is must be done outside the office, considering the current condition that the company apply shift work WFH and WFO.

j. *User* dilarang untuk melakukan perubahan pengaturan internet yang telah dilakukan, kecuali dengan ijin Kepala Divisi Teknologi Informasi dan Departemen Pengawas Keamanan Informasi dan Risiko Sistem.

j. User is prohibited to change internet setting without approval from Information Technology Division and Information Security and System Risk Controller Department.

k. User dilarang untuk meminjam dan/atau meminjamkan *User ID* dan *Password user* lain untuk menggunakan Internet

k. User is prohibited to borrow and/or lend User ID and Password from other user to use Internet.

2. Risiko Penyalahgunaan Fasilitas Internet

2. Risk of Internet Misuse

a. Penyalahgunaan akses Internet dapat mengakibatkan risiko virus dan keamanan karena penurunan kinerja jaringan, mengakibatkan kerusakan pada jaringan dan/atau PC bahkan mengganggu kegiatan operasional.

a. Misuse of Internet access can cause risk of virus and security that will impact to network performance, network and/or PC disturbance, even affecting operational activity.

b. Untuk meminimalkan risiko *social engineering* lakukan *clear cookies /history/cache* secara rutin.

b. To minimize social engineering risk, clear cookies/history/cache on regular basis.

c. User dilarang untuk mengakses Internet secara terus-menerus. Tujuannya adalah untuk menjaga kinerja jaringan dan meminimalkan kemungkinan *hacker* untuk menyimpan informasi *IP address* bank.

c. User is prohibited to access Internet all the time. The purpose is to maintain network performance and minimize hacker possibility in gaining Bank IP address.

d. Melakukan *download* dan *install illegal software* sehingga dapat menimbulkan risiko hukum terkait lisensi.

d. Prohibited to download and install illegal software that can cause legal risk related to license.

e. Informasi dari internet yang digunakan untuk tujuan bisnis dan tidak diverifikasi terlebih dahulu dapat menimbulkan risiko reputasi.

e. Unverified information from the Internet is potential to raising reputation risk.

3. Menyaring Informasi dari Internet

3. Filtering Information from Internet

a. *Filter* informasi dilakukan berdasarkan

a. Filtering information is base on risk

kebutuhan dan tingkat risiko dalam mengamanankan jaringan dan kepentingan Bank.

b. Jika laporan *filter* akses jaringan menunjukkan informasi tersebut mempunyai risiko terhadap keamanan jaringan Bank, maka Departemen Pengawas Keamanan Informasi dan Kontrol Risiko Sistem memberikan rekomendasi kepada Divisi TI untuk langkah antisipasinya.

level and requirement to secure network and Bank reputation.

b. If report of network access filtering shown risk to Bank network, then Information Security and System Risk Controller Department give recommendation to IT Division for anticipation.

4. Pertahanan Terhadap Internal *Cyber Crime*

a. Melakukan *review* dan analisa terkait standar akses kontrol dan standar klasifikasi data untuk menghindari akses yang tidak sesuai.

b. Manajemen memberikan tindakan disiplin yang berefek jera kepada setiap karyawan yang melakukan kejahatan/penipuan/pencurian atau kejahatan lain yang melanggar kebijakan dan peraturan perundang-undangan yang berlaku

4. Defense for Internal Cyber Crime

a. Review and analysis of standard access control and standard data classification to prevent unauthorized access.

b. Management give disciplinary that has impact to employee who conduct crime/fraud/theft or other crime that violate policy or regulation.

5. Pertahanan Terhadap External *Cyber Crime*

a. Sistem *Administrator/* Departemen Perencanaan Teknologi Informasi atau penanggung jawab keamanan jaringan komunikasi harus orang yang mempunyai kualifikasi dan telah mendapatkan pelatihan yang cukup, baik mengenai keamanan jaringan, kemungkinan risiko-risiko, serta mengerti bagaimana caranya membangun suatu sistem keamanan yang baik.

b. Melakukan sosialisasi, *awareness* atau *training* terkait keamanan jaringan untuk meminimalkan risiko *cyber crime*.

c. Melakukan penyaringan setiap *file* yang masuk melalui Internet berdasarkan pada kriteria tertentu dan tingkat risiko.

5. Defense for External Cyber Crime

a. System Administrator / Information Technology Planning Department or network communication PIC is a qualified person and get adequate training about network security, risk and how to design a good network security system.

b. Conduct socialization, awareness or training for network security to minimize cyber crime risk.

c. Filtering each file from Internet base on specific criteria and risk level.

6. Pertahanan Terhadap Opportunis *Cyber Attack*

Opportunistic Cyber Crime adalah suatu upaya kejahatan yang dilakukan karena melihat adanya celah/kelemahan dalam pertahanan,

6. Defense for Opportunist Cyber Attack

Opportunist Cyber Crime is a fraud attempt because of security weakness exploitation, not because of intentional penetration.

bukan semata-mata sengaja mencari celah/kelemahan itu sendiri.

a. Menerapkan teknik kombinasi akses kontrol dan prosedur untuk meminimalkan opportunis *cyber crime*.

b. Sistem Administrator/ Departemen Perencanaan Teknologi Informasi bertanggung jawab membangun suatu pertahanan yang memadai dan berusaha me*review* setiap sistem pengamanan yang sudah ada sehingga dapat lebih disempurnakan dari waktu ke waktu.

c. Menerapkan manajemen risiko yang efektif terhadap suatu proses dalam sistem, untuk mengidentifikasi kelemahan pertahanan keamanan informasi yang dimiliki sebelum adanya kejadian serangan.

7. Pertahanan Terhadap *DoS Attack*

Serangan *Denial of Service* (DoS): serangan internet terhadap *website* dimana *client* tidak dapat menggunakan salah satu pelayanan yang ada di *website* tersebut sebagaima mestinya. Dalam beberapa kasus dapat menurunkan *performance*. Dalam kasus yang lebih buruk lagi *server* menjadi *overload* dan dapat menyebabkan *crash* pada sistem.

a. Sistem *Administrator* / Departemen Perencanaan Teknologi Informasi harus dapat mendeteksi, membaca dan mengklarifikasi jenis serangan serta menentukan langkah yang harus dilakukan untuk mengatasinya/ meminimalisasi.

b. *Contigency Plan* terhadap serangan DoS harus dipelihara dan diuji secara berkala untuk memastikan kesesuaiannya.

c. Sistem Administrator/ Departemen Perencanaan Teknologi Informasi harus memiliki kemampuan dan pelatihan (*training*) yang memadai sehingga jika terjadi serangan, proses pemulihan bisa dilakukan secara cepat.

8. Pertahanan Terhadap *Hacker Attack*

Hacker atau *Stealth*: orang yang mencari kelemahan suatu sistem dan mencari keuntungan dari kelemahan sistem yang ditemukan. Contoh dari serangan ini misalnya, *stealth bomb, logic bomb, trojan horse* dan

a. Implement access control combination and procedure to minimize opportunist cyber crime.

b. System Administrator/ Information Technology Planning Department responsible to design adequate security and review security system for future development and improvement.

c. Implement an effective risk management to identify information security weakness before attack happen.

7. Defense for DoS Attack

Denial of Service attack: attacking website in order to make client cannot use website function. On specific case to decrease performance. On worst case making server overload and causing system crash.

a. System Administrator / Information Technology Planning Department detecting, review and clarify attack type include define action to minimize and solve problem.

b. Contingency Plan of DoS attack is maintained and tested on regular basis to ensure its suitability.

c. System Administrator / Information Technology Planning Department is capable and have adequate training in order to give quick response during attack.

8. Defense for Hacker Attack

Hacker or Stealth: People who search system weakness and get advantage the system. Example: stealth bomb, logic bomb, trojan, and other malicious software.

perangkat lunak perusak lainya.

a. Mengembangkan kesadaran dan kewaspadaan seluruh karyawan serta memasang alat atau sistem pencegahan yang sesuai untuk meminimalkan risiko.

b. Sistem Administrator/ Departemen Perencanaan Teknologi Informasi harus membangun suatu sistem pertahanan memadai terhadap kemungkinan serangan dari *hacker/stealth* dan dapat melindungi seluruh aset informasi yang dimiliki oleh perusahaan.

c. Manajemen memberikan fasilitas berupa *training* mengenai kewaspadaan terhadap serangan *hacker* termasuk upaya-upaya yang dapat dilakukan dalam mencegah/meminimalkan serangan.

d. Risiko terkait serangan *hacker*, misalnya:

   1) *Malware* dapat melakukan duplikat dirinya sendiri dan mungkin di-*download* dan dieksekusi tanpa disadari sehingga dapat merusak sistem.

   2) *Email* yang diterima mungkin mengandung *malware* dan menyebar ke semua alamat dalam sistem *email* perusahaan pada saat dibuka sehingga dapat mengakibatkan kerusakan data, kerusakan sistem dan data penerima.

   3) Replikasi *malware* tersebut tidak hanya terbatas pada perusahaan tetapi juga dapat berdampak pada penerima *email* seperti rekan bisnis dan Nasabah sehingga dapat menurunkan reputasi perusahaan.

9. Mengumpulkan Bukti *Cyber Crime*

   a. Sistem Administrator/ Departemen Perencanaan Teknologi Informasi dan Departemen Pengawas Keamanan Informasi dan Kontrol Risiko Sistem bertanggung jawab mengumpulkan bukti-bukti kejahatan *cyber crime* dan melaporkan hasil temuan tersebut ke Komite Pengarah TI untuk ditindaklanjuti. Meskipun demikian seluruh karyawan juga diminta waspada dan melaporkan setiap kejadian yang ditemukannya termasuk

a. Improve awareness and caution of all employees and install security system to minimize risk.

b. System Administator / Information Technology Planning Department design security system to prevent attack from hacker/stealth and to protect information asset owned by company.

c. Management give training facility of security awareness includes efforts to prevent/minimize attack

d. Risk related to hacker attack:

   1) Malware can duplicate and possible to be downloaded and execute without intentional, and cause system failure

   2) Email may contain malware and spread to all company email and cause data corrupt, system corrupt, and receiver data

   3) Malware replicate is not limited to company but may impact to email user such as business partner and customer, which cause company reputation.

9. Collecting Evidence of Cyber Crime

   a. System Administator/ Information Technology Planning Department and Information Security and System Risk Controller Department responsible to collect evidence of cyber crime and report finding to Information Technology Steering Committee for next action. Nevertheless all employee should aware and report all cyber crime incident and evidence.

mengumpulkan bukti-bukti kejahatan *cyber crime*.

b. Jika informasi rahasia yang dimiliki harus diserahkan ke pihak ketiga/pihak berwenang dalam upaya melakukan tuntutan secara hukum maka harus dipastikan bahwa keamanan data/informasi tersebut sudah dilindungi dengan baik dalam kontrak/perjanjian dan telah mendapat persetujuan dari Direksi.

b. Confidential information is delivered to third party/authorized party in the term of legal action, the data/information should be protected using agreement and after get approval from Board of Directors.

10. Meminimalkan Pengaruh *Cyber Attack*

a. Sistem Administrator / Departemen Perencanaan Teknologi Informasi mempunyai *problem handling* terkait *cyber attack*, melakukan pemeliharaan sistem dan jaringan, melakukan *backup* serta uji coba *recovery* yang teratur untuk meminimalkan risiko *cyber crime*.

b. Membuat *contigency plan* agar kegiatan bisnis tetap dapat berjalan.

10. Minimize Cyber Attack Impact

a. System Administrator/ Information Technology Planning Department have problem handling related to cyber attack, maintain system and network, conduct backup and testing recovery in order to minimize cyber crime risk.

b. Create contingency plan to maintain business continuity.

B. *Intranet*

1. Aturan Penggunaan *Web Browser*

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 otentikasi / verifikasi yaitu dengan menggunakan *User ID* dan *password*.

B. Intranet

1. Procedure of Web Browser Usage

a. All employees is prohibited to use web browser outside work related. The purpose is to prevent virus, trojan, and malicious software. Virus can penetrate the security that activated via web browser.

b. Application via web browser should use authentication / verification process, by using user ID and password.

2. Situs Web Bank

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

a. Divisi Planning dan Finance dalam hal ini Departemen *Corporate Secretary* berkoordinasi dengan Departemen Perencanaan Teknologi Informasi untuk

2. Bank Website

Website is tools to promote product and as information source for Bank.

a. Planning and Finance Division in this case Corporate Secretary Department coordinate with Information Technology Planning Department to select a qualified

memilih *vendor* yang berkualitas untuk pembuatan *website*, pengembangan dan pemeliharaan berdasarkan izin Direksi.

vendor for website design, development, and maintenance base on Director Approval.

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

b. Website update base on Website Management Policy and each update process is documented and reviewed on regular basis.

c. 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*.

c. Website officer is responsible to update website information and responsible to the information integrity.

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

d. Information at website should be protected from data steal include in the maintenance process.

e. Departemen Perencanaan Teknologi Informasi bertanggung jawab untuk melakukan *backup* terhadap *website* secara keseluruhan termasuk databasenya secara berkala satu bulan sekali setiap akhir bulan 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 risiko dengan tersedianya *backup* tersebut.

e. Information Technology Planning Department is responsible for backup the website as a whole including database once a month at the end of month to anticipate attacks on website (eg re-routing address, defacing the display, etc), so tha recovery website can be done as soon as possible and minimize risk with the availability of these backup.

C. *Email*

C. Email

1. Fasilitas *email* hanya diberikan kepada *user* berdasarkan kepentingan pekerjaannya.

1. Email facility only used by user for work related.

2. Fungsi Operasional dan Dukungan Teknologi Informasi bertanggung jawab untuk pembuatan alamat *email* dan konfigurasi *email* berdasarkan *user form* dan formulir BRP-CS-56 Pernyataan Pendaftar Fasilitas *email* atau Internet.

2. Operational Function and Technology Information Support is responsible to create email address and email configuration base on request form and BRP-CS-56 Statement For E-mail and Internet Facility Applicant.

3. Setting *quota mailbox* dapat berubah sesuai dengan kebutuhan dan berdasarkan pada pertimbangan tertentu dalam hal ini adalah terkait dengan level jabatan. Perubahan quota *mailbox* dapat ajukan dengan cara membuat *request* melalui Intramart . Berikut adalah rincian setting

3. Mailbox quota can be changed base on requirement or other consideration related of job position. For Changes user can be request via intramart. Following is detail setting of mailbox quota :

quota mailbox :

a. Staff – 100 MB

b. Kepala Departemen – 256 MB

c. Kepala Divisi / Cabang – 358 MB

d. Dewan Komisaris / Direksi – 512 MB

4. *Email* keluar dan *email* masuk dengan lampiran memiliki batasan maksimal total sebesar 10 MB dan kecuali *email* masuk dari Regulator (OJK, BI, PPATK, dll).

5. Penggunaan *email* secara bersama-sama dalam satu Divisi / Departemen / Cabang dapat dilakukan dengan menggunakan alamat *email* khusus. Masing-masing Kepala Divisi / Departemen / Cabang bertanggung jawab untuk mengawasi penggunaan *email* tersebut.

6. Penggunaan email publik yang digunakan oleh Divisi / Departemen tertentu untuk kepentingan pekerjaan diperbolehkan dan Divisi / Departemen terkait bertanggung jawab penuh atas email tersebut.

7. Dilarang untuk melakukan pendaftaran pada *website* / *group* / *milis* tertentu kecuali untuk kepentingan pekerjaan dengan persetujuan Kepala Divisi Teknologi Informasi dan Departemen Keamanan Informasi dan Kontrol Risiko Sistem.

8. Dilarang untuk menggunakan *email* perusahaan untuk keperluan pribadi.

9. Informasi / data pekerjaan yang berhubungan dengan perusahaan / pekerjaan dilarang dikirim ke alamat *email* pribadi dengan alasan dan maksud apapun. Misalnya dengan alasan untuk menyelesaikan pekerjaan kantor dirumah kemudian mengirimkan ke *email* (Yahoo!, Google) dan lain-lain

10. Jika berdasarkan monitoring dan *review* yang dilakukan oleh Departemen Pengawas Keamanan Informasi dan Kontrol Risiko Sistem ditemukan hal-hal yang dianggap berbahaya bagi perusahaan, maka fasilitas *email* dapat dihapus / diblokir.

11. Dilarang untuk melakukan konfigurasi *email* pada perangkat pribadi (misalnya

a. Staff – 100 MB

b. Department Head – 256 MB

c. Division / Branch Head – 358 MB

d. BOC/BOD – 512 MB

4. Outgoing email and Incoming email with attachment has a maximum total limit 10MB except incoming email from Regulator (OJK, BI, PPATK, ect).

5. Email sharing at one Division/Department/Branch can be done by using a special email address. Each Head of Division / Department / Branch responsible to supervise email usage.

6. Public email used by Division / Department for work purposes is allowed and that Division / Department are fully responsible for that email.

7. Prohibited to register at website/group/mailing list other than work related and with approval from Head of Information Technology Division and Information Security and System Risk Controller Department.

8. Prohibited to use company email for personal purpose.

9. Information / data related to work/company is prohibited to sent to personal email. Example to finish work at home then send to Yahoo!, Google and other email.

10. If base on monitoring and review from Information Security and System Risk Controller Department found a potency to disturb company information the email facility may be revoked / blocked.

11. Prohibited to configure email at personal tools (such as mobile phone, Blackberry,

mobile phone, blackberry, *Mobile Tablet*, dan lain-lain), kecuali pada perangkat yang disediakan oleh perusahaan dan berdasarkan persetujuan Departemen Pengawas Keamanan Informasi dan Kontrol Risiko Sistem .

Mobile Tablet, other), except at tools that given by the company and base on approval from Information Security and System Risk Controller Department.

12. Beberapa *file* lampiran pada *email* di blokir untuk meminimalkan risiko (misalnya *executable file*, mp3, mov, dan lain-lain), jika *file* tersebut diperlukan untuk tujuan pekerjaan maka berdasarkan persetujuan Departemen Pengawas Keamanan Informasi dan Kontrol Risiko Sistem dapat dikirim / diterima.

12. Some of attachment at email is blocked to minimize risk (such as executable file, mp3, mov, and other) if file is require for work purpose, then base on Information Security and System Risk Controller Department can be sent/received.

13. Untuk *user* yang sedang cuti / *training* dapat mengaktifkan *auto respond email* sendiri.

13. User that on leave/training may activate auto respond email by them self.

14. Setiap *user* bertanggung jawab dalam menghapus *email* yang sudah tidak diperlukan pada *file sent / deleted item* untuk menjaga kapasitas *email*.

14. User responsible to delete unused email at sent/deleted item folder to maintain email capacity.

15. Alamat tujuan *email* dikelola dan dikontrol oleh *user* sendiri.

15. Email address is maintained and controlled by user itself.

16. Untuk menghindari virus yang diaktifkan melalui format html, disarankan user sebaiknya menggunakan format *plain text* dan menghindari membuka / klik lampiran / isi *email* yang mencurigakan.

16. To prevent virus that activate via html, user should use plain text format and avoid open/click a suspicious attachment/body email.

17. Lampiran informasi / data yang akan dikirimkan melalui *email* harus menggunakan *password*. *Password* untuk membuka lampiran *email* harus dikirim melalui *email* terpisah atau melalui sarana lain seperti telepon, sesuai dengan SOP *Information Leakage Prevention*.

17. Attachment of information/data that is send using email, whether for internal and external must use password. Password to open email attachment must be sent by separated email or by other method such as by phone, in accordance with the Information Leakage Prevention Procedure.

18. Pastikan kembali bahwa lampiran yang akan dikirimkan sudah benar dan menggunakan *password*.

18. Make sure that attachment to be sent is correct and use password.

19. Pengiriman *email* keluar hanya dapat dilakukan jika sudah di-*approve* oleh Kepala Divisi ,sedangkan untuk Kantor Cabang hanya dapat dilakukan jika sudah di-*approve* oleh Kepala Cabang Apabila Kepala Divisi sedang berhalangan / tidak ditempat, maka *approval* untuk pengiriman *email* dilakukan oleh *Director in Charge*.

19. Sending email need approval by Head of Division, for Branch Office need approval from Branch Head. If Head of Division was absent/not available,then approval for sending email performed by Director in Charge.

20. Hindari menuliskan banyak alamat *email* pada field CC (*Carbon Copy*), karena hal tersebut dapat memenuhi *inbox* penerima (*email chain*). Selalu pastikan bahwa penerima yang tercantum dalam field CC mengerti / terkait dengan tujuan / pembahasan *email* tersebut.

20. Avoid input many address at field CC (Carbon Copy), this will flood inbox. Always ensure that the receiver in the CC understand/related to the email subject.

21. Jika akan mengirim ke lebih dari satu alamat penerima, gunakan *field* BCC (*Blind Carbon Copy*) untuk mencegah alamat *email* yang bersifat pribadi menyebar ke pihak lainnya.

21. If will send to more than one receiver, use field BCC (Blind Carbon Copy) to prevent email address spread.

22. *Undisclosed Recipient* harus didaftarkan terlebih dahulu ke Departemen Pengawas Keamanan Informasi dan Kontrol Risiko Sistem .

22. Undisclosed Recipient is registered first to Information Security and System Risk Controller Department.

23. Untuk keperluan *monitoring* dan meminimalkan risiko terkait *email*, dalam mengirimkan *email* setiap karyawan menyertakan Kepala Divisi / Departemen / Cabang dan *Director in charge* dalam *field* CC.

23. For monitoring and to minimize risk, in sending email all employee must involve Head of Division/Department/Branch and Director in Charge in CC field.

24. Untuk mengirimkan *broadcast email* keluar dengan banyak penerima digunakan aplikasi *Email Blast*

24. To send outgoing email broadcasts with multiple recipients used Email Blast application.

25. Jenis *broadcast email* keluar yang menggunakan aplikasi *Email Blast* adalah :

    a. *Email* yang dikirimkan kepada lebih dari satu penerima (Nasabah).
    b. Isi *email* adalah informasi yang berisi pemberitahuan atau informasi dan bersifat satu arah.
    c. Informasi yang dikirimkan ke Nasabah bukan informasi rahasia Nasabah ataupun informasi rahasia Bank.

25. The type of broadcast email using Email Blast application :

    a. Email send to more than one recipient (Customer).
    b. The content of email is information that contains notice or information and is one way.
    c. Information send to the Customer is not about Customer confidential information or the Bank confidential information.

26. Untuk pemeliharaan alamat *email* Nasabah di aplikasi *Email Blast* dilakukan oleh Divisi terkait (*Helpdesk Internet Banking*, Divisi Treasury, Divisi *Business Development)*

26. For maintenance of Customer email address at Email Blast application conduct by related Division (Helpdesk Internet Banking, Treasury Division, Business Development Division)

27. Pemilik *email* diwajibkan untuk menggunakan *signature file* dalam setiap *email* yang berisi identitas pengirim, peringatan, dan *disclaime*r, seperti

27. Email address must using signature file at each email that contains sender identity, disclaimer such as

Jhon Kerry
IT Planning Department – IT Division

Jhon Kerry
IT Planning Department – IT Division

Bank Resona Perdania

PT Bank Resona Perdania
Jakarta Mori Tower
30th, 31st and 32nd Floor
Jl. Jend. Sudirman Kav. 40-41,
Bendungan Hilir, Tanah Abang
Jakarta Pusat 12010
Indonesia

Phone: +62-21-570-1958 Ext. 31069
Fax : +62-21-570-1936
Email : jhon@perdania.co.id
Web : www.perdania.co.id

PT Bank Resona Perdania
Jakarta Mori Tower
30th, 31st and 32nd Floor
Jl. Jend. Sudirman Kav. 40-41,
Bendungan Hilir, Tanah Abang
Jakarta Pusat 12010
Indonesia

Phone: +62-21-570-1958 Ext. 31069
Fax : +62-21-570-1936
Email : jhon@perdania.co.id
Web : www.perdania.co.id

Important Notice: This email message is intended for the named recipient only. It may be privileged and/or confidential. If you are not the intended named recipient of this email then you should not copy it or use it for any purpose, nor disclose its contents to any other person. You should contact PT. Bank Resona Perdania as shown above so that we can take appropriate action at no cost to yourself. Unless otherwise specifically stated by the sender, any documents or views presented are solely those of the sender and do not constitute official documents or views of PT. Bank Resona Perdania. If you have received this communication in error, please notify us immediately by responding to john@perdania.co.id or by telephone. PT. Bank Resona Perdania is neither liable for the proper and complete transmission of the information contained in this communication nor for any delay in its receipt

Warning: Although this email has been scanned for the possible presence of computer viruses prior to dispatch, we cannot be held responsible for any viruses or other material transmitted with, or as part of, this email without our knowledge

IV. PENGENDALIAN INTERNAL

A. Audit Internal

Dalam rangka memastikan keamanan penggunaan internet dan *email*, audit wajib dilakukan tahunan oleh pihak independen baik Auditor Intern maupun Auditor Ekstern.

Cakupan audit antara lain mencakup:

1. Kinerja internet dan *email*
2. Akses logik
3. Akses fisik
4. *Remote access*
5. Infrastuktur
6. Dokumentasi

IV. INTERNAL CONTROL

A. Internal Audit

In order to ensure use of internet and email security, audit mandatory to be done annually by independent party, either Internal Audit or External Audit.

Audit covering:

1. Internet and Email performance
2. Logical access
3. Physical access
4. Remote access
5. Infrastructure
6. Documentation

V. PENUTUP

Pedoman Internet dan *Email* 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.

Pedoman ini mulai berlaku sejak memperoleh persetujuan Presiden Direktur tanggal 16 Juni 2023 dan mencabut Pedoman Internet dan *Email* edisi 3, Juni 2021.

Pedoman Internet dan *Email* 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 Internet and Email Guideline is published in 2 (two) languanges, namely Indonesia and English, and if there are differences in interpretation between the two, then the reference is Indonesia.

This guideline comes into force since obtaining the approval of the President Director on June 16, 2023 and revokes the internet and E-mail Guideline 3rd edition, June 2021.

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