LAPORAN KEPATUHAN SEMESTERAN
TIM SMKI ISO 27001:2022
PT BPR BATUARTOREJO
No Dok. FR.02.00/PND.02.00/601786001/VIII/2023
Laporan Semester I 2025

*BPR/BPRS cukup mengisi pada kolom terpenuhi atau tidak, jika terpenuhi ketik "1" jika tidak ketik"0"

** Kolom referensi pendukung merupakan contoh pilihan bukti pendukung yang dapat/ telah dimiliki oleh BPR BPRS

BUTIR-BUTIR PENILAIAN			
NO	INDIKATOR	TERPENUHI=1, TIDAK = 0	Bukti Audit(Catatan/ Dokumen/ Foto)
A. Aspek Dokumentasi	Mempunyai Dokumen PKS dengan Ditjen Dukcapil yang masih berlaku	1	No 100.47.1/15432 /DUKCAPIL. No 96/BAR/DUKCAPIL/X/2023
	Mempunyai Dokumen Juknis Dukcapil yang masih berlaku	1	027/2813/IDKN
	Membuat Surat Pernyataan Tanggung Jawab Mutlak (SPTJM) yang dikeluarkan oleh Ditjen Dukcapil	1	FR.01-SOP-08/DITJEN-DUKCAPIL
	MembuatSurat Pernyataan NDA (Non Disclosure Aggrement) yang dikeluarkan Ditjen Dukcapil	1	FR.01-SOP-08/DITJEN-DUKCAPIL
	Mengisi dan mengirimkan Formulir Berlangganan Sharing Bandwidth Jaringan Bersama ke Perbarindo	1	67/BAR/DUKCAPIL/IX/2018
	Membuat Surat Pernyataan Penggunaan Sharing Bandwith Jaringan Bersama serta NDA	1	FR.01/SOP.04.00/PND.02.00/(601786)/VIII/2023
	Membuat Surat Pernyataan Penjagaan Kerahasiaan Informasi (NDA) untuk pengguna Sharing Bandwith Jaringan Bersama dan Card Reader	1	FR.01/SOP.04.00/PND.02.00/(601786)/VIII/2023
	Mengirimkan Berita Acara Implementasi Sharing Bandwith	0	Nihil
	Mengirimkan Daftar Nama Tim SMKI sesuai dengan anggota yang ada.	1	FR.03.00/PND.01.00/601786/VIII/2023
	Mendukumentasikan hasil review yang dilakukan oleh TIM SMKI	0	Nihil
B. Aspek Operasional	Menetapkan dan menyetujui Kebijakan SMKI.	1	
	Mengimplementasikan Kebijakan, Paduan Sistem dan Teknis Keamanan Data dan Informasi Perbarindo	1	**SOP.01.00/PND.01.00/601786/VIII/2023**
	Menetapkan dan menyetujui SOP Pengendalian Dokumen terdokumentasi	1	**SOP.01.00/PND.01.00/601786/VIII/2023**
	Menetapkan dan menyetujui SOP Manajemen Aset	1	SOP.02.00_PND.01.00_601786_VIII_2023

Menetapkan dan menyetujui SOP Manajemen Insiden	1	SOP.04.00_PND.02.00_601786_VIII_2023- Manajemen Insiden BPR BPRS
Menetapkan dan menyetujui SOP Audit Internal	1	SOP.05.00_PND.01.00_601786_VIII_2023- Audit Internal BPR_BPRS
Menetapkan dan menyetujui SOP Tinjauan Manajemen	1	SOP.06.00_PND.01.00_601786_VIII_2023 - Tinjauan Manajemen BPR_BPRS
Menetapkan dan Menyetujui Juknis SMKI	0	Nihil
Menempatkan lokasi APAR pada lokasi yang mudah dijangkau dan strategis		
Konsisten menerapkan kebijakan meja bersih dan layar bersih	1	
Menggunakan Sistem Operasi (Windows) yang original	0	
Menerapkan kebijakan pengamanan pada Windows dengan penguncian otomatis dalam waktu 5 menit setelah tidak aktif.	1	
Memasang kamera pengawas (CCTV) di lokasi strategis	1	
Menyediakan kunci keamanan tempat penyimpanan aset dan data informasi	0	

	Menyediakan Mesin Penghancur Kertas	1	
C. Aspek Teknis	Mematuhi Panduan Jaringan Bersama	0	
	Mengupdate Daftar User dan Hardware yang digunakan	0	
	Surat Permohonan Pernonaktifan Admin Lama & Permintaan Admin baru aplikasi Sharing	0	
	Mengupdate Log Incident jika ada insiden atau gangguan.	0	
	Melakukan penghancuran Data/Aset IT (jika ada) sesuai ketentuan	0	
	Pengecekan Antivirus Setiap Bulan (antivirus aktif dan update)	0	
D. Aspek Pelaporan	Mengirimkan Laporan Pergantian/Penambahan User	0	
	Membuat dan mengirimkan Pakta Integritas atas pegawai yang baru bergabung/menjabat	0	
	Mengirimkan laporan Hasil Tinjauan Manajemen	0	
E. Aspek Kepatuhan	Komitmen manajemen terhadap implementasi ISO 27001:2022 dengan Kebijakan dan Kualitas Keamanan Informasi dapat diumumkan pada situs web atau diunggah dalam bentuk piagam yang ditempatkan di lokasi yang mudah dilihat	0	
	Komitmen manajemen untuk meningkatkan kompetensi karyawan, dibuktikan dengan surat edaran yang menyatakan bahwa semua karyawan pengguna / anggota Tim SMKI wajib melakukan awareness ISO 27001:2022	0	
	Komitmen manajemen untuk meningkatkan kompetensi karyawan, dibuktikan dengan surat edaran yang menyatakan bahwa Pejabat Audit Internal wajib melakukan awareness ISO 19011:2018	0	
	Membuat dan mengirimkan Laporan Kepatuhan.	0	

Aspek	Jumlah	Skor	Total Nilai
A. Aspek Dokumentasi	7	**77,77777778**	
B. Aspek Operasional	10	**71,42857143**	
C. Aspek Teknis	0	**0**	**29,84126984**

D. Aspek Pelaporan	0	**0**	
E. Aspek Kepatuhan	0	**0**	

Batu, 15 Juli 2025

Dibuat oleh,

Wahyudin
Tim SMKI

PT. BPR BATUARTOREJO * BATU *

Disetujui oleh,

Ichwanul Ridwan S.E., Ak.
Direksi

PT BANK PERKREDITAN RAKYAT
BATU ARTOREJO

Standard Operating Procedure (SOP)

PENGENDALIAN INFORMASI TERDOKUMENTASI AKSES DATA DUKCAPIL

Nomor Dokumen	:	SOP.01.00/PND.01.00/601786/VIII/2023
Tanggal Terbit	:	10 Agustus 2023
Revisi	:	00
Klasifikasi	:	TERBATAS

PENGESAHAN
P.T. B.P.R. BATU ARTOREJO BATU
Ichwanul Ridwan SE., Ak.
DIREKTUR

PT BANK PERKREDITAN RAKYAT
BATU ARTOREJO

Standard Operating Procedure (SOP)

PENGENDALIAN INFORMASI TERDOKUMENTASI AKSES DATA DUKCAPIL

Nomor Dokumen	:	SOP.01.00/PND.01.00/601786/VIII/2023
Tanggal Terbit	:	10 Agustus 2023
Revisi	:	00
Klasifikasi	:	TERBATAS

PENGESAHAN
P.T. B.P.R. BATU ARTOREJO BATU
Ichwanul Ridwan SE., Ak.
DIREKTUR

RIWAYAT PERUBAHAN

Rev.	Tanggal	Bagian	Alasan Perubahan

A. TUJUAN :

Memastikan hanya dokumen SMKI khusus untuk data akses dukcapil beserta lampiran yang terkini dan sah tersedia di semua unit kerja yang memerlukan serta menetapkan penanganan dan pemeliharaan dokumen dan rekaman (bukti hasil) mulai dari penyimpanan, perlindungan, masa simpan sampai dengan pemusnahannya.

B. RUANG LINGKUP :

Penerbitan, revisi, pengesahan, pemberian identitas, dan pendistribusian dokumen data akses dukcapil. Penyimpanan, perlindungan, masa simpan bukti hasil sampai dengan pemusnahannya serta penanganan dokumen rahasia.

C. DEFINISI DAN KETENTUAN

- Dokumen adalah ketentuan tertulis yang digunakan secara resmi sebagai pedoman dalam penerapan SMKI pada organisasi.
- Dokumen Internal adalah Kebijakan, Pedoman, Standar operasional prosedur (SOP) dan dokumen lain disusun berdasarkan peraturan perundangan dan pedoman-pedoman eksternal yang berlaku yang diterapkan dilingkungan organisasi.
- Dokumen Eksternal adalah dokumen yang berasal dari luar organisasi yang dijadikan acuan untuk melakukan suatu pekerjaan atau kegiatan, Seperti undang-undang, Peraturan Pemerintah, Peraturan Daerah, *Manual Book*/Ketentuan/*Guidance*, dan lain-lain.
- Dokumen Induk adalah dokumen acuan yang memiliki beberapa turunan dokumen lainnya.

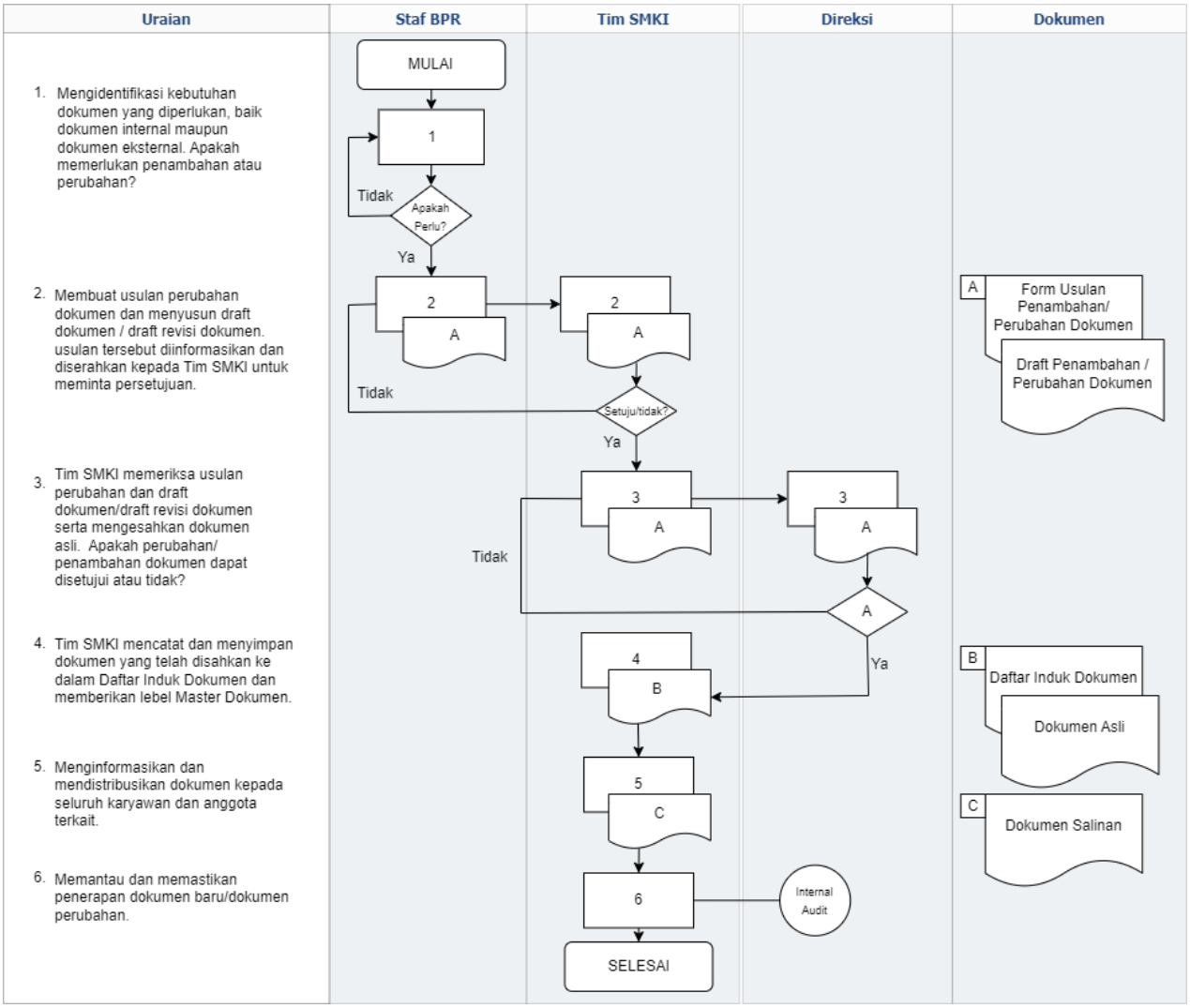
D. REFERENSI :

- SNI ISO/IEC 27001:2022
- Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi;
- Surat Edaran Dirjen Disdukcapil No. 400.8/11759/Dukcapil tanggal 8 Agustus 2023 tentang Tanggapan atas Surat Perbarindo Perihal ISO 27001.
- Surat Edaran Dirjen Disdukcapil No. 470/15017/Dukcapil tanggal 26 September 2022 tentang Perlindungan Data Kependudukan Dalam Keamanan Informasi.
- Surat Dirjen Dukcapil No. 470/17431/DUKCAPIL tanggal 24 September 2018 tentang Pemberitahuan Atas Konsep Sharing Bandwidth Komunikasi Data Perbarindo.
- POJK Republik Indonesia No. 8 Tahun 2023 tentang Penerapan Program Anti Pencucian Uang, Pencegahan Pendanaan Terorisme Dan Pencegahan Pendanaan Proliferasi Senjata Pemusnahan Massal di Sektor Jasa Keuangan.

E. PENANGGUNG JAWAB :

- Tim SMKI

F. ALUR PROSES



G. RINCIAN PROSEDUR :

- **PROSEDUR PENGENDALIAN DOKUMEN AKSES DUKCAPIL**

1. Penerbitan / Revisi Dokumen

   Identifikasi kebutuhan dokumen baru maupun penambahan/revisi dokumen SMKI dilakukan oleh Staf Bagian administrasi kredit dengan memberikan form usulan dengan melampirkan draft dokumen kepada Tim SMKI.

2. Pengesahan Dokumen

   Dokumen yang baru atau dokumen yang direvisi harus ditinjau kembali oleh Tim SMKI serta disetujui dan disahkan oleh Direksi dengan menandatangani kolom tanda-tangan yang disiapkan.

   - Pemberian Identitas BPR/BPRS

     Pemberian nomor dokumen yang sudah di berikan Perbarindo cukup ditambahkan kode sandi BPR/BPRS dari OJK.

     Maka penerapan di PT BPR Batu Artorejo menjadi : SOP.01.00/PND.01.00/PERB-SMKI/601786001/VIII/2023.

Kode	Uraian
PND	Panduan
SOP	Standar Operasional Prosedur
FR	Formulir
01	Urutan Dokumen
00	Urutan Revisi
PERB-SMKI	Tim SMKI Perbarindo
601786	Kode Sandi BPR
VIII	Bulan Terbit
2023	Tahun Terbit

     Note : Format Penomoran Dokumen dari perbarindo tidak boleh diubah oleh BPR/BPRS.

   - Pelabelan Dokumen

     Pelabelan dokumen ditetapkan menjadi 3 kategori yaitu: Master Dokumen, Salinan dokumen dan Obsolete.

1. Master Dokumen adalah Dokumen asli yang menjadi acuan pada setiap Salinan dokumen yang didistribusikan. Master dokumen dikendalikan oleh pengendali dokumen oleh Tim SMKI.
2. Salinan Dokumen adalah Dokumen yang didistribusikan.
3. Obsolete Dokumen adalah Dokumen yang sudah tidak digunakan dan didistribusikan.

KETERANGAN

1. NOMOR REVISI

- Dokumen yang pertama kali terbit diberi nomor 00. Selanjutnya jika terjadi revisi menjadi 01, 02 dan seterusnya hingga n. Jika terjadi perubahan nama dokumen maka diterbitkan edisi baru.
- Daftar induk dan distribusi dokumen serta status revisinya dicatat dalam form pemantauan dokumentasi.

2. DISTRIBUSI DOKUMEN

- Tim SMKI mendistribusikan dokumen kepada Staf BPR/BPRS dengan identitas nomor salinan sesuai yang tercantum dalam Daftar Induk dan Distribusi Dokumen dengan mengisi formulir Distribusi Dokumen.
- Distribusi untuk Perbarindo/pihak lain menggunakan Surat Pengantar.
- Staf BPR/BPRS tidak diizinkan untuk menggandakan dan mendistribusikan dokumen SMKI yang diterimanya tanpa persetujuan Direksi.
- Pencatatan pada form pemantauan dokumentasi.

3. PENYIMPANAN DAN PEMUSNAHAN DOKUMEN

- Setiap penerima dokumen wajib menyimpan, menjaga dan memelihara dokumen tersebut dengan sebaik-baiknya dan harus tersedia apabila dibutuhkan.
- Tim SMKI menyimpan master dokumen.
- Pencatatan pada form pemantauan dokumentasi

4. **DOKUMEN YANG SUDAH TIDAK BERLAKU**

Setiap dokumen yang sudah tidak berlaku wajib ditarik dan dimusnahkan sesuai ketentuan masa retensi oleh Tim SMKI dan disetujui Direksi. Pelaksanaan pemusnahan dokumen dicatat pada form pemantauan dokumentasi.

5. **MASA SIMPAN DOKUMEN**

Masa simpan dokumen di PT BPR Batu Artorejo diatur berdasarkan kategori sebagai berikut :

- Dokumen SMKI terkait data akses dukcapil dikategorikan sebagai dokumen dengan masa simpan selama 5 (lima) tahun.

- **PROSEDUR PENGENDALIAN BUKTI HASIL**

1. Penyusun dokumen SMKI dibuat pemantauan dokumentasi dalam form yang memuat:

a. Jenis dokumen eksternal atau internal, jika eksternal dikendalikan dan segera diadaptasikan. Jika internal segera disosialisasikan.
b. Tipe dokumen berupa Panduan, Standar Operasional Prosedur (SOP), Instruksi Kerja, Form dan Rekaman.
c. Nama Dokumen
d. Agenda berupa revisi, penerbitan, pemusnahan, pengesahan, distribusi
e. Tanggal pelaksanaan agenda
f. Kerahasiaan dokumen, apakah bersifat rahasia atau tidak
g. Masa Simpan
h. Penanggung jawab dokumen

2. Dokumen disimpan oleh Tim SMKI, di tempat yang terlindung agar terhindar dari kerusakan, kehilangan serta mudah diakses apabila diperlukan.

3. Pemusnahan Bukti hasil setelah memenuhi masa simpan dokumen dan harus mendapatkan persetujuan Direksi dengan menggunakan form pemantauan dokumentasi.

H. Dokumen terkait

1. Form Pengendalian Dokumen FR.01.00/PND.01.00/601786/VIII/2023
2. Form Usulan Revisi Dokumen FR.02.00/PND.01.00/601786/VIII/2023

3. Form Distribusi Dokumen FR.03.00/PND.01.00/601786/VIII/2023

PT BANK PERKREDITAN RAKYAT
BATU ARTOREJO

Standard Operating Procedure (SOP)

MANAJEMEN ASET UNTUK AKSES DATA DUKCAPIL

Nomor Dokumen	:	SOP.02.00/PND.01.00/601786/VIII/2023
Tanggal Terbit	:	10 Agustus 2023
Revisi	:	00
Klasifikasi	:	TERBATAS

PENGESAHAN
P.T. B.P.R. BATU ARTOREJO · BATU ·
Ichwanul Ridwan SE., Ak.
DIREKSI

RIWAYAT PERUBAHAN

Rev.	Tanggal	Bagian	Alasan Perubahan

A. TUJUAN :

Kebijakan Pengendalian Pengelolaan Aset Informasi ini bertujuan untuk memberi acuan dalam mengelola perlindungan keamanan yang memadai akan aset informasi PT. BPR BATU ARTOREJO dan memastikan bahwa aset informasi memiliki tingkat perlindungan keamanan yang sesuai dengan klasifikasinya yang terhubung dengan aplikasi jaringan Bersama Perbarindo untuk mengakses data dukcapil.

B. RUANG LINGKUP :

Kebijakan Pengendalian Pengelolaan Aset Informasi ini meliputi:

1. Pengklasifikasian aset informasi yang terhubung Aplikasi jaringan Bersama untuk mengakses data dukcapil;
2. Acuan dalam penyusunan SOP dan/atau petunjuk teknis Pengelolaan Aset Informasi yang terhubung pada Aplikasi jaringan Bersama untuk mengakses data dukcapil.

C. DEFINISI DAN KETENTUAN

- Inventaris Aset Informasi merupakan kegiatan untuk melakukan pendataan, pencatatan, dan pelaporan hasil pendataan aset.
- Aset Informasi adalah merupakan aset dalam bentuk data atau dokumen, perangkat lunak, aset fisik, dan aset tak berwujud.

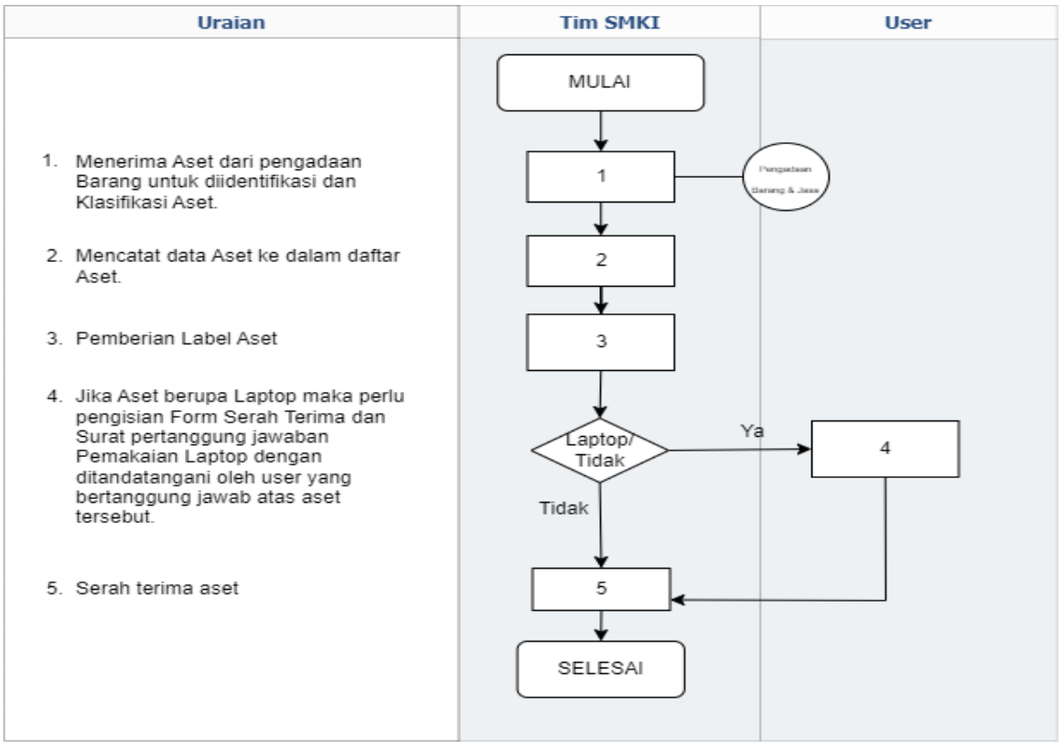
D. REFERENSI :

- SNI ISO/IEC 27001:2022
- Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi;
- Surat Edaran Dirjen Disdukcapil No. 400.8/11759/Dukcapil tanggal 8 Agustus 2023 tentang Tanggapan atas Surat BPR/BPRS Perihal ISO 27001.
- Surat Edaran Dirjen Disdukcapil No. 470/15017/Dukcapil tanggal 26 September 2022 tentang Perlindungan Data Kependudukan Dalam Keamanan Informasi.
- Surat Dirjen Dukcapil No. 470/17431/DUKCAPIL tanggal 24 September 2018 tentang Pemberitahuan Atas Konsep Sharing Bandwidth Komunikasi Data BPR/BPRS.
- POJK Republik Indonesia No. 8 Tahun 2023 tentang Penerapan Program Anti Pencucian Uang, Pencegahan Pendanaan Terorisme Dan Pencegahan Pendanaan Proliferasi Senjata Pemusnahan Massal di Sektor Jasa Keuangan.

E. PENANGGUNG JAWAB :

- Tim SMKI

F. ALUR PROSES :



G. RINCIAN PROSEDUR :

Hal-hal yang harus diperhatikan dalam pengendalian pengelolaan aset informasi adalah sebagai berikut:

a. Pengelolaan daftar inventaris aset informasi yang berisi seluruh aset informasi utama seperti perangkat lunak, perangkat keras, dan layanan TIK yang terhubung dengan aplikasi jaringan Bersama untuk akses data dukcapil akan dilindungi dan harus secara jelas mengidentifikasi setiap aset, pemilik aset, dan lokasinya. Pengelolaan dan perawatan berdasarkan Daftar Inventaris Aset Informasi dilakukan oleh Staf BPR yang ditunjuk.

b. Seluruh serah terima aset wajib menggunakan formulir serah terima no FR.002.00/SOP.002.00/601786/XI/2022 yang dibuat oleh staf Pejabat Audit Internal dan mematuhi segala aturan yang ada. Khusus untuk Laptop, ditambah dengan Surat Pernyataan Pertanggung jawaban Penggunaan Laptop dan wajib mematuhi peraturan penggunaan laptop di luar kantor.

c. Pengguna Aset Informasi bertanggung jawab untuk melakukan perlindungan terhadap keamanan seluruh aset informasi yang berada di bawah pengawasannya;

d. Kebijakan dan aturan penggunaan aset-aset informasi ditetapkan dan berlaku bagi seluruh pegawai dan pihak ketiga. Seluruh pengguna aset informasi tanpa kecuali harus mematuhi kebijakan dan aturan yang telah ditetapkan dan harus melaporkan kepada Tim SMKI apabila terjadinya pelanggaran terhadap kebijakan ini.

Kebijakan yang berlaku dalam pengklaslfikasian aset informasi adalah sebagai berikut:

a. Aset-aset informasi utama digolongkan berdasarkan nilai, ketentuan/kebutuhan kegiatan yang menggunakannya, tingkat kerahasiaan, dan tingkat kerawanannya bagi BPR/BPRS. Klasifikasi aset informasi dilakukan oleh Staff Teknologi Informasi dan disetujui oleh atasan langsungnya;

   1. Pemberian label pada aset informasi harus dilakukan secara konsisten pada aset informasi BPR/BPRS yang pelaksanaannya mengacu pada Petunjuk Teknis Pengelolaan Aset Informasi.
   2. Aset informasi yang diterima dari pihak ketiga harus memuat dan mencantumkan klasifikasinya atau dilakukan penggolongan ulang sesuai aturan yang ditetapkan BPR/BPRS.
   3. Aset informasi berupa bukti hasil penting milik BPR/BPRS harus dilindungi dari kehilangan, kerusakan, atau penyalahgunaan sesuai peraturan yang berlaku oleh pemilik aset.

B. Petunjuk Teknis Pengelolaan Aset Informasi mengatur hal-hal sebagai berikut:

1. Inventarisasi aset informasi;
2. Pemberian label;
3. Pengiriman informasi:
4. Penyimpanan informasi;
5. Penggunaan informasi.

KLASIFIKASI	KETERANGAN
RAHASIA	Informasi yang membutuhkan pengamanan tinggi/ketat dan hanya boleh diketahui oleh Direksi dan/atau pegawai tertentu yang ditetapkan. Informasi rahasia adalah informasi yang dapat menimbulkan Risiko yang tinggi apabila terjadi kebocoran antara lain: • Kerugian finansial yang besar, • Terganggunya layanan Sistem Elektronik dalam jangka lama, atau • Menimbulkan reputasi yang buruk <u>Termasuk kategori ini antara lain</u>: Rencana Bisnis (*Business Plan*), data pegawai, hasil penilaian kinerja pegawai, network, log system administrator, dan rahasia lainnya.

TERBATAS	Informasi yang telah terdistribusi di lingkungan internal, yang penyebarannya secara internal tidak memerlukan persetujuan dari pemilik informasi. Risiko kebocoran informasi secara tak berwenang ke pihak luar berkategori menengah, tidak sebesar risiko informasi berklasifikasi "Rahasia" Termasuk kategori ini antara lain: Kebijakan dan prosedur, laporan audit (internal/eksternal), hasil kajian risiko, catatan rapat internal dan laporan operasional layanan yang tidak bersifat "Rahasia", rencana investasi/anggaran, dokumen kontrak.
BIASA	Informasi yang tidak memerlukan pengamanan dari aspek kerahasiaan atau informasi yang secara sengaja disediakan bagi publik. Termasuk kategori ini antara lain: Brosur layanan dan situs publik layanan Sistem Elektronik dan informasi lainnya yang disediakan bagi publik.

C. Penanganan aset informasi

Informasi atau aset yang digunakan untuk menyimpan dan/atau memproses informasi pada organisasi harus terdata oleh Tim SMKI dan disetujui oleh pimpinan agar tidak ada aset yang terbawa oleh SDM yang telah berhenti bekerja. Ketentuan penanganan penyimpanan, transmisi, pemusnahan informasi sesuai dengan klasifikasinya ditetapkan oleh Tim SMKI, baik untuk dokumen tercetak maupun dokumen dalam bentuk softcopy.

Penanganan aset fisik yang sudah tidak digunakan dapat dilakukan dengan cara:

1. Dimusnahkan dengan cara dibakar dan dihancurkan. Pemusnahan asset dengan cara ini wajib melalui persetujuan Direksi dan dibuatkan Berita Acara Pemusnahan Aset dengan memastikan seluruh data/informasi sudah tidak ada atau sudah di backup. Proses pemusnahan wajib didokumentasikan dan menjadi lampiran berita acara.
2. Dijual sesuai dengan cara yang sudah ditetapkan dengan peraturan tersendiri yang dibuat oleh manajemen PT BPR Batu Artorejo. Penjualan Asets harus dengan persetujuan Direksi. Sebelum asets yang terkait dengan akses data dukcapil dijual, maka semua data informasi yang ada didalamnya harus dimusnahkan terlebih dahulu.

Untuk asset softcopy dan software disimpan dalam hard disk eksternal dengan jangka waktu tertentu untuk perlindungan informasi. Hard disk eksternal disimpan dalam tempat yang telah ditentukan.

Penggunaan removable media dikendalikan oleh masing-masing pengguna perangkat

sehingga ketika hilang tidak ada data yang bocor, pengguna perangkat harus terdata pada daftar aset informasi sehingga penelusuran mudah dilakukan. Media penyimpan informasi ketika dimusnahkan dipastikan bahwa informasi yang pernah tersimpan didalamnya tidak dapat di retrieve kembali.

D. Software yang diizinkan

PT BPR BATU ARTOREJO mengizinkan untuk pemasangan software pada Aset hardware berupa laptop atau PC yang digunakan untuk akses data dukcapil sebagai berikut:

1. Microsoft Office series
2. Microsoft Edge
3. Microsoft OneDrive
4. Aplikasi Printer (Epson, HP, Canon dan lain lain)
5. Foxit Reader
6. Mozilla Firefox
7. Whatsapp
8. Winamp
9. WinRAR
10. Zoom
11. BPR EKTP Sharing Bandwidth
12. Windows PC Health Check
13. Windows Defender
14. McAfee
15. dan software lainnya yang berhubungan dengan pengembangan teknologi.

E. Domain yang diizinkan

BPR/BPRS mengizinkan untuk pemasangan akun domain email pada aset hardware berupa laptop/PC sbb:

1. yahoo.com
2. gmail.com

B. FORMULIR :

1.	Daftar Aset	FR.01.00/SOP.002.00/601786/VIII/2023
2.	Formulir Serah Terima Aset	FR.02.00/SOP.002.00/601786/VIII/2023
3.	Berita Acara Pemusnahan Aset	FR.03.00/SOP.02.00/601786/VIII/2023

PT BANK PERKREDITAN RAKYAT
BATU ARTOREJO

Standard Operating Procedure (SOP)
MANAJEMEN INSIDEN
AKSES DATA DUKCAPIL

Nomor Dokumen	:	SOP.04.00/PND.02.00/601786/VIII/2023
Tanggal Terbit	:	10 Agustus 2023
Revisi	:	00
Klasifikasi	:	TERBATAS

PENGESAHAN
Ichwanul Ridwan SE., Ak. DIREKTUR

RIWAYAT PERUBAHAN

Rev.	Tanggal	Bagian	Alasan Perubahan

A. TUJUAN :

Manajemen Insiden ini disusun untuk memberi acuan terhadap terjadinya gangguan yang diakibatkan oleh User dan Perangkat yang ada di BPR/BPRS yang terhubung ke jaringan bersama Perbarindo untuk mengakses data Dukcapil.

B. RUANG LINGKUP :

Kebijakan insiden manajemen ini mencakup hal-hal sebagai berikut:

1. Terjadinya Insiden pada kesalahan user
2. Terjadinya Insiden pada kondisi perangkat
3. Terjadinya Insiden pada jaringan internet

C. DEFINISI

1. Insiden adalah suatu gangguan yang tidak terencana di dalam mengakses data kependudukan melalui Jaringan Bersama Perbarindo.
2. Manajemen Insiden adalah suatu proses untuk pencegahan akan terjadinya gangguan yang disebabkan kesalahan user, kondisi perangkat, dan jaringan internet.

D. REFERENSI :

1. SNI ISO/IEC 27001:2022
2. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi;
3. Surat Edaran Dirjen Disdukcapil No. 400.8/11759/Dukcapil tanggal 8 Agustus 2023 tentang Tanggapan atas Surat Perbarindo Perihal ISO 27001.
4. Surat Edaran Dirjen Disdukcapil No. 470/15017/Dukcapil tanggal 26 September 2022 tentang Perlindungan Data Kependudukan Dalam Keamanan Informasi.
5. Surat Dirjen Dukcapil No. 470/17431/DUKCAPIL tanggal 24 September 2018 tentang Pemberitahuan Atas Konsep Sharing Bandwidth Komunikasi Data Perbarindo.
6. POJK Republik Indonesia No. 8 Tahun 2023 tentang Penerapan Program Anti Pencucian Uang, Pencegahan Pendanaan Terorisme Dan Pencegahan Pendanaan Proliferasi Senjata Pemusnahan Massal di Sektor Jasa Keuangan.

E. PENANGGUNG JAWAB :

Tim SMKI

F. KETENTUAN

1. Ketentuan pengguna :
    a. Wajib menandatangani Surat Pernyataan dan NDA Pengguna Jaringan Bersama Perbarindo.
    b. Penggunaan kredensial akun (User ID dan Password) bersifat rahasia, tidak diperkenankan untuk dipindahtangankan.
    c. Apabila terjadi pergantian user admin maka harus mendapatkan persetujuan dari Direksi.
2. Standar perangkat (PC/Laptop) yang digunakan dalam instalasi aplikasi jaringan bersama Perbarindo adalah sebagai berikut :
    - Wajib terinstal Sistem Operasi Windows 10 - 64 bit
    - Memiliki kapasitas RAM 4GB
    - Memiliki kapasitas Hardisk 128 GB
    - Memiliki Processor Core 2 Duo
3. Standar jaringan internet yang digunakan dalam mengakses aplikasi jaringan bersama Perbarindo adalah sbb:
    a. Minimal Bandwidth 20 Mbps untuk 5 perangkat yang digunakan untuk mengakses jaringan bersama Perbarindo.
    b. Ketersediaan koneksi jaringan sesuai dengan waktu operasional kantor.

G. RINCIAN PROSEDUR :

H.1. PENGGUNA

1. LUPA PASSWORD USER OPERATOR
    a. Klik menu lupa password pada aplikasi
    b. Mengecek kode verifikasi pada email
    c. memasukan kode verifikasi dan password baru pada aplikasi

2. LUPA PASSWORD USER ADMIN
    a. Klik menu lupa password secara mandiri melalui menu lupa password pada aplikasi
    b. Mengecek kode verifikasi pada email
    c. Memasukan kode verifikasi dan password baru pada aplikasi
    d. Apabila user admin gagal melakukan reset password, maka user admin wajib menginformasikan kepada tim SMKI untuk ditindaklanjuti.
    e. Tim SMKI mencatat insiden pada log insiden kemudian membuat surat permohonan reset password untuk disetujui direksi.
    f. Direksi menyetujui surat permohonan reset password.
    g. Surat yang telah disetujui dikirimkan kepada DPP Perbarindo oleh Staf yang ditunjuk.

3. PENGGANTIAN USER ADMIN
   Resign/Berhenti bekerja/Cuti/Pindah Jabatan
   a. Tim SMKI membuat surat permohonan penggantian dan penonaktifan user admin untuk disetujui direksi.
   b. Direksi menyetujui surat permohonan penggantian dan penonaktifan user admin.
   c. Surat yang telah disetujui dikirimkan kepada DPP Perbarindo oleh Staf yang ditunjuk.

H.2. PERANGKAT

KERUSAKAN/KEHILANGAN PERANGKAT

a. Tim SMKI mencatat pada log insiden dan menginformasikan kepada direksi terkait info kerusakan/kehilangan perangkat.
b. Tim SMKI membuat surat permohonan penonaktifan terminal dengan menginformasikan Nomor Serial perangkat kepada user admin apabila yang Rusak/hilang adalah perangkat operator.
c. Apabila perangkat yang hilang adalah perangkat admin maka, mengajukan kepada Perbarindo untuk menonaktifkan perangkat dengan Nomor Serial perangkat tersebut.

H.3 JARINGAN

JARINGAN INTERNET MATI/TIDAK STABIL

a. Tim SMKI mencatat gangguan jaringan internet pada log insiden untuk identifikasi permasalahan tersebut.
b. Apabila gangguan tidak dapat diatasi, maka Tim SMKI menghubungi Internet Service Provider (ISP).

H. FORMULIR :

- Log Insiden – FR.03.00/SOP.02.00/PND.02.00/601786/VIII/2023

PT BANK PERKREDITAN RAKYAT
BATU ARTOREJO

Standard Operating Procedure (SOP)

AUDIT INTERNAL
PROGRAM KERJA TIM SMKI

Nomor Dokumen	:	SOP.05.00/PND.01.00/601786/VIII/2023
Tanggal Terbit	:	10 Agustus 2023
Revisi	:	00
Klasifikasi	:	TERBATAS

PENGESAHAN
P.T. B.P.R. BATU ARTOREJO BATU Ichwanul Ridwan SE., Ak. DIREKSI

RIWAYAT PERUBAHAN

Rev.	Tanggal	Bagian	Alasan Perubahan

A. TUJUAN :

Prosedur ini disusun untuk mengatur pelaksanaan Audit Internal terhadap Program Tim SMKI.

B. RUANG LINGKUP :

Prosedur ini digunakan sebagai dasar Pelaksanaan Audit terhadap program kerja SMKI yang telah disusun oleh tim SMKI dan disetujui oleh Direksi minimal meliputi :

1. Tindak lanjut tindakan koreksi atas audit tahun lalu
2. Audit terhadap program kerja tim SMKI yang telah disetujui direksi
3. Audit terhadap tindaklanjut dari insiden manajemen (daftar log insiden).

C. DEFINISI

- Ketidaksesuaian adalah tidak terpenuhinya persyaratan yang berkaitan dengan tujuan yang telah ditentukan.
- Ketidaksesuaian Minor adalah ketidaksesuaian yang tidak memiliki dampak yang serius terhadap sistem mutu,
- Ketidaksesuaian Major adalah ketidaksesuaian yang memiliki potensi dapat menghasilkan dampak yang serius terhadap pencapaian sistem pencapaian mutu.
- Peluang Observasi adalah sebuah saran dengan tujuan untuk peningkatan.

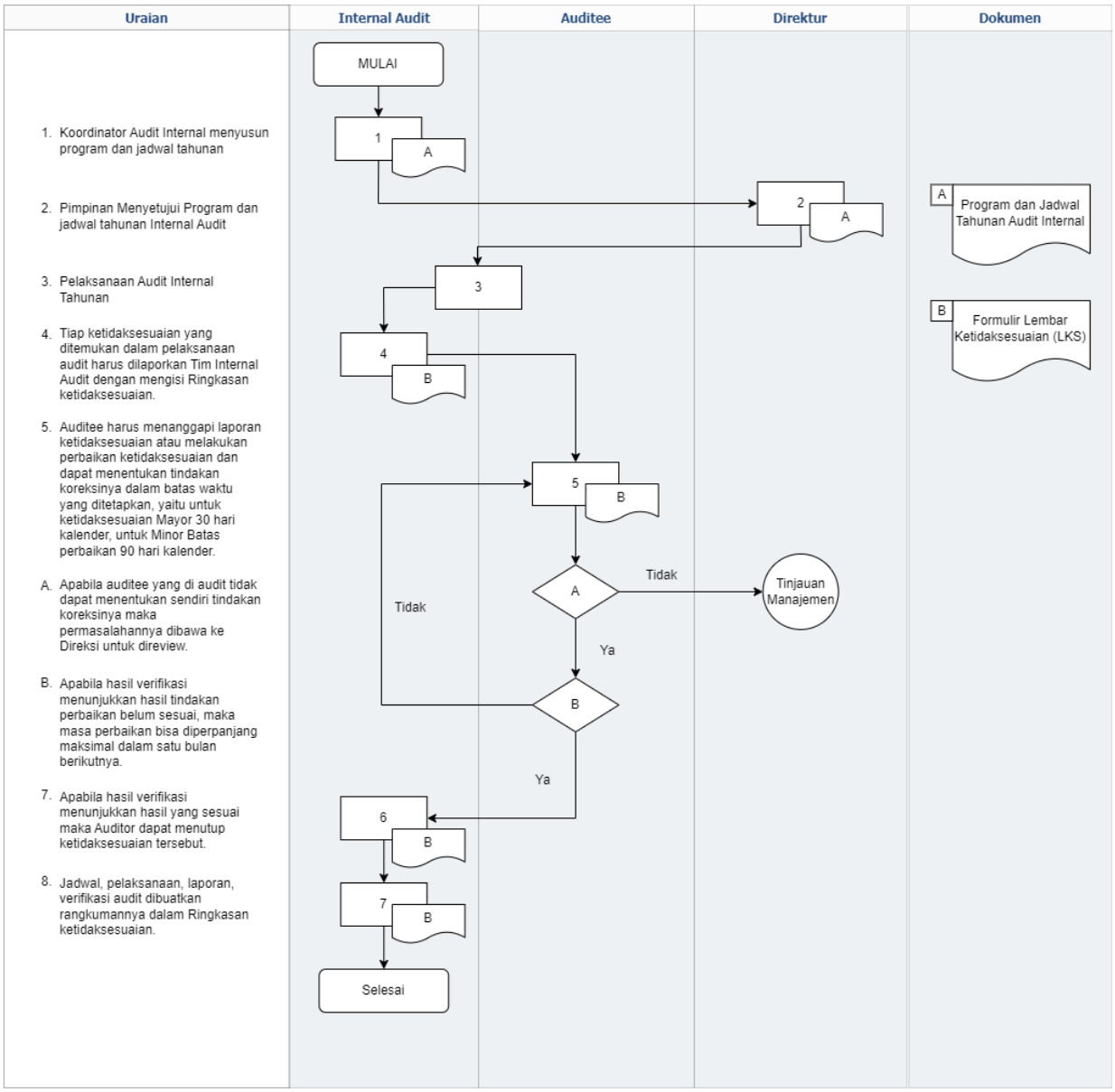
D. REFERENSI :

a. SNI ISO/IEC 27001:2022
b. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi;
c. Surat Edaran Dirjen Disdukcapil No. 400.8/11759/Dukcapil tanggal 8 Agustus 2023 tentang Tanggapan atas Surat Perbarindo Perihal ISO 27001.
d. Surat Edaran Dirjen Disdukcapil No. 470/15017/Dukcapil tanggal 26 September 2022 tentang Perlindungan Data Kependudukan Dalam Keamanan Informasi.
e. Surat Dirjen Dukcapil No. 470/17431/DUKCAPIL tanggal 24 September 2018 tentang Pemberitahuan Atas Konsep Sharing Bandwidth Komunikasi Data Perbarindo.
f. POJK Republik Indonesia No. 8 Tahun 2023 tentang Penerapan Program Anti Pencucian Uang, Pencegahan Pendanaan Terorisme Dan Pencegahan Pendanaan Proliferasi Senjata Pemusnahan Massal di Sektor Jasa Keuangan.

E. PENANGGUNG JAWAB :

- Direksi dan Auditor Internal

F. ALUR PROSES



G. RINCIAN PROSEDUR :

1. Koordinator Audit Internal menyusun program dan jadwal tahunan untuk audit internal berdasarkan skala prioritas dengan persetujuan Direksi. Program dan jadwal disahkan oleh Direksi.
2. Dalam jangka waktu setahun semua bagian yang terkait dengan SMKI sudah diaudit dan audit harus mencakup semua Program Tim SMKI.
3. Auditor Internal merupakan PE Audit Internal/SKAI BPR/BPRS dan tidak boleh mengaudit unit kerjanya sendiri untuk menghindari konflik kepentingan dan komitmen integritas audit.
4. Auditor adalah seorang yang pernah mendapat pelatihan dalam hal mengaudit dan pelatihan (Minimal pemahamanan) terkait skema/kriteria/standar yang akan diaudit.
5. Auditor menyediakan daftar periksa audit sebelum melakukan audit.
6. Setiap ketidaksesuaian yang ditemukan dalam pelaksanaan audit harus dilaporkan dengan mengisi Ringkasan ketidaksesuaian.
7. Ketidaksesuaian berupa Mayor didefinisikan dapat menghambat jalannya Program SMKI sehingga mengancam keberlangsungan bisnis dan berdampak kerugian material.
8. Ketidaksesuaian Minor didefinisikan tidak mempengaruhi kemampuan Tim SMKI mencapai hasil namun apabila tidak ditindaklanjuti berpotensi menjadi mayor.
9. Peluang perbaikan / Observasi merupakan rekomendasi/saran perbaikan terhadap Program yang perlu dipertimbangkan pemenuhannya dikarenakan berpotensi menjadi minor.
10. Auditee harus menanggapi laporan ketidaksesuaian dan dapat menentukan tindakan koreksinya dalam batas waktu yang ditetapkan, yaitu untuk ketidaksesuaian Minor 30 hari kalender, untuk Mayor Batas perbaikan 90 hari kalender.
11. Apabila auditee yang di audit tidak dapat menentukan sendiri tindakan koreksinya maka permasalahannya dibawa ke Direksi untuk direview.
12. Apabila hasil verifikasi menunjukkan hasil tindakan perbaikan belum sesuai, maka masa perbaikan bisa diperpanjang maksimal dalam satu bulan berikutnya.

13. Apabila hasil verifikasi menunjukkan hasil yang sesuai maka Auditor dapat menutup ketidaksesuaian tersebut.
14. Jadwal, pelaksanaan, laporan, verifikasi audit dibuatkan rangkumannya dalam Ringkasan ketidaksesuaian.
15. Auditor Internal melaporkan hasil audit internal dan disampaikan dalam Rapat Tinjauan Manajemen.

H. FORMULIR :

1.	Form Program Internal Audit	FR.01.00/SOP.05.00/PND.01.00/601786/VIII/2023
2.	Form Jadwal Internal Audit	FR.02.00/SOP.05.00/PND.01.00/601786/VIII/2023
3.	Form Ceklis Internal Audit	FR.03.00/SOP.05.00/PND.01.00/601786/VIII/2023
4.	Form Laporan Internal Audit	FR.04.00/SOP.05.00/PND.01.00/601786/VIII/2023
5.	Form LKS Internal Audit	FR.05.00/SOP.05.00/PND.01.00/601786/VIII/2023

PT BANK PERKREDITAN RAKYAT
BATU ARTOREJO

Standard Operating Procedure (SOP)

TINJAUAN MANAJEMEN
PROGRAM KERJA TIM SMKI

Nomor Dokumen	:	SOP.06.00/PND.01.00/601786/VIII/2023
Tanggal Terbit	:	10 Agustus 2023
Revisi	:	00
Klasifikasi	:	TERBATAS

PENGESAHAN
P.T. B.P.R. BATU ARTOREJO BATU **Ichwanul Ridwan SE., Ak.** **DIREKTUR**

RIWAYAT PERUBAHAN

Rev.	Tanggal	Bagian	Alasan Perubahan

A. TUJUAN :

- Melakukan interaksi antara semua tingkatan yang relevan untuk Keamanan Informasi BPR/BPRS. Tanggung jawab individu dan kelompok ditetapkan untuk mendapatkan bukti hasil, melaporkan dan menyampaikan data dan informasi yang terkait dengan akses data dukcapil
- Sebagai pedoman dalam pelaksanaan dan memberikan tanggapan tinjauan manajemen dari Program Tim SMKI yang terkait dengan akses data dukcapil

B. RUANG LINGKUP :

Tinjauan manajemen yang mencakup persiapan, pelaksanaan dan tindak lanjut, agar seluruh informasi dan kendala yang dihadapi dalam penerapan SMKI dapat ditinjau sehingga dapat ditingkatkan efektifitasnya dan memenuhi persyaratan Penyelenggaraan Sistem Pengendalian Internal.

C. DEFINISI

- Notulen Tinjauan Manajemen adalah catatan resmi dari tinjauan manajemen yang berisikan siapa, apa, bagaimana dan hasil dari suatu hal yang dirapatkan atau disidangkan.
- Stakeholder adalah seluruh pihak yang memiliki hubungan dan kepentingan.
- Tim SMKI adalah Tim Keamanan Sistem Manajemen Keamanan Informasi yang berfungsi sebagai kontrol keamanan yang telah disesuaikan dengan kebutuhan organisasi.

D. REFERENSI :

a. SNI ISO/IEC 27001:2022

b. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi;

c. Surat Edaran Dirjen Disdukcapil No. 400.8/11759/Dukcapil tanggal 8 Agustus 2023 tentang Tanggapan atas Surat Perbarindo Perihal ISO 27001.

d. Surat Edaran Dirjen Disdukcapil No. 470/15017/Dukcapil tanggal 26 September 2022 tentang Perlindungan Data Kependudukan Dalam Keamanan Informasi.

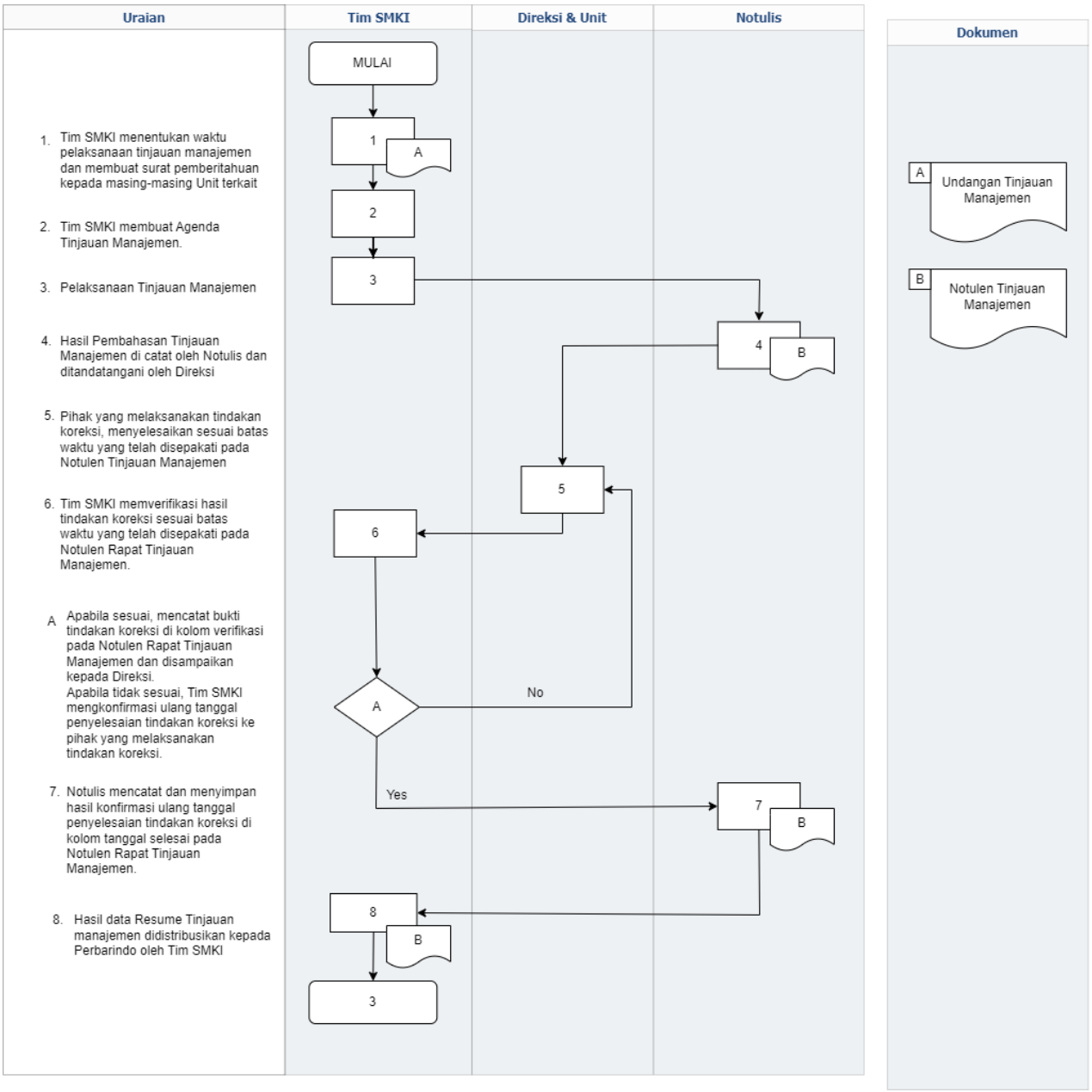
e. Surat Dirjen Dukcapil No. 470/17431/DUKCAPIL tanggal 24 September 2018 tentang Pemberitahuan Atas Konsep Sharing Bandwidth Komunikasi Data Perbarindo.

f. POJK Republik Indonesia No. 8 Tahun 2023 tentang Penerapan Program Anti Pencucian Uang, Pencegahan Pendanaan Terorisme Dan Pencegahan Pendanaan Proliferasi Senjata Pemusnahan Massal di Sektor Jasa Keuangan.

E. PENANGGUNG JAWAB :

a. Direksi bertanggung jawab melaksanakan, memimpin dan memberikan tanggapan terhadap input masalah tinjauan manajemen, dan menetapkan rekomendasi tinjauan manajemen.
b. Staf BPR/BPRS yang ditunjuk untuk bertanggung jawab menyiapkan agenda (input) tinjauan manajemen, mengkoordinir pelaksanaan kegiatan serta mengendalikan rekaman tinjauan manajemen.
c. Tim SMKI bertanggung jawab terhadap pelaksanaan komunikasi internal pada lingkupnya serta memberikan saran dan masukan serta melaksanakan rekomendasi dari tinjauan manajemen yang terkait tanggung jawabnya.

F. ALUR PROSES



G. RINCIAN PROSEDUR :

1. Tinjauan manajemen dilaksanakan minimal satu kali dalam setahun.
2. Ketua Tim SMKI BPR/BPRS membuat agenda pembahasan tinjauan manajemen yang mencakup hal-hal berikut ini:
   a. Status Tindak Lanjut Hasil Rapat Tinjauan Manajemen yang terakhir
   b. Hasil Internal Audit
   c. Rencana tindak lanjut Penyelesaian hasil internal audit dengan menyebutkan tanggal penyelesaian dan PIC.
3. Hasil pembahasan Rapat Tinjauan Manajemen dicatat oleh notulis dalam Notulen tinjauan manajemen dan ditandatangani oleh Direksi BPR/BPRS.
4. Pihak yang melaksanakan tindakan koreksi, menyelesaikan sesuai batas waktu yang telah disepakati pada Notulen Tinjauan Manajemen. Ketua SMKI memverifikasi hasil tindakan koreksi sesuai batas waktu yang telah disepakati pada Notulen Rapat Tinjauan Manajemen. Apabila sesuai, mencatat bukti tindakan koreksi di kolom verifikasi pada Notulen Rapat Tinjauan Manajemen dan disampaikan kepada Pimpinan organisasi. Apabila tidak sesuai, Tim SMKI mengkonfirmasi ulang tanggal penyelesaian tindakan koreksi ke pihak yang melaksanakan tindakan koreksi.
5. Notulis mencatat dan menyimpan hasil konfirmasi ulang tanggal penyelesaian tindakan koreksi di kolom tanggal selesai pada Notulen Rapat Tinjauan Manajemen.
6. Salinan Notulen Tinjauan manajemen dikirimkan ke Perbarindo

H. FORMULIR :

1. Notulen Tinjauan Manajemen FR.01.00/SOP.06.00/PND.01.00/601786/VIII/2023
2. Format undangan Tinjauan manajemen FR.02.00/SOP.06.00/PND.01.00/601786/VIII/2023
3. Presensi Kehadiran Tinjauan Manajemen FR.03.00/SOP.06.00/PND.01.00/601786/VIII/2023

SURAT KEPUTUSAN
DIREKSI PT BPR BATU ARTOREJO

TENTANG

PENUNJUKAN TIM SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI), SERTA TUGAS DAN TANGGUNG JAWAB

PT BANK PERKREDITAN RAKYAT
BATU ARTOREJO

NOMOR DOKUMEN	:	FR.03.00/PND.01.00/601786/VIII/2023
TANGGAL TERBIT	:	10 Agustus 2023
REVISI	:	00
KLASIFIKASI	:	TERBATAS

SURAT KEPUTUSAN
No.SK.01.00/PND.02.00/PERB-SMKI/601786/VIII/2023

TENTANG
PENUNJUKAN TIM SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI),
SERTA TUGAS DAN TANGGUNG JAWAB

Menimbang :

1. Dalam rangka menjamin kerahasiaan, keutuhan, dan ketersediaan informasi untuk mewujudkan tata kelola yang baik, perlu menerapkan standar IS0 27001:2022 Mengenai sistem manajemen keamanan informasi secara konsisten dan berkesinambungan terhadap seluruh kegiatan penggunaan jaringan Bersama perbarindo untuk mendukung layanan perbankan di lingkungan PT. BPR BATU ARTOREJO
2. Bahwa berdasarkan pertimbangan sebagaimana di maksud pada poin 1 perlu untuk menetapkan keputusan tentang pembentukan TIM Pelaksanaan Sistem Manajemen Keamanan Informasi berbasis ISO 27001:2022.
3. Bahwa nama yang tercantum pada keputusan ini dipandang memenuhi syarat untuk diangkat sebagai tim implementasi SMKI (Tim SMKI).

Mengingat :

1. Surat Edaran Dirjen Disdukcapil No. 400.8/11759/Dukcapil tanggal 8 Agustus 2023 tentang Tanggapan atas Surat BPR/BPRS Perihal ISO 27001.

Memutuskan :

1. Membentuk dan mengangkat Tim SMKI dengan susunan personil yang terlibat terdapat dalam keputusan ini

Menetapkan Susunan Tim SMKI sebagai berikut :

1. **KETUA TIM**
   a. Syarat Kompetensi :
      - Min. Pendidikan SMA/SMK
      - Telah mengikuti Pelatihan ISO 27001:2022
      - Telah bekerja di PT BPR BATU ARTOREJO minimal selama 1 tahun.
      - Mampu memahami annex control pada ISO 27001:2022.
      - Memiliki kemampuan Leadership dalam pengelolaan project
      - Memiliki kemampuan dalam perencanaan penerapan sistem

   b. Tugas dan wewenang :
      - **Tugas :**
        a. Melaksanakan tanggung jawab dan kewenangan yang melekat pada Top Management terkait penerapan SMKI ISO 27001:2022 di PT BPR/BPRS;
        b. Melaporkan kinerja SMKI ISO 27001:2022 untuk peluang untuk peningkatan, khususnya kepada Top Management;
        c. Mengkoordinasi pelaksanaan Audit Internal yang terkait dengan SMKI berikut pelaporannya kepada PERBARINDO.
        d. Memutuskan penyelesaian setiap masalah terkait dengan penerapan SMKI ISO 27001:2022 di PT BPR BATU ARTOREJO yang tidak dapat diselesaikan.
      - **Wewenang :**
        Memiliki akses terhadap Sistem Manajemen Keamanan Informasi maupun Dokumen SMKI

2. **ANGGOTA**
   a. Syarat Kompetensi :
      - Min. Pendidikan SMA/SMK
      - Telah mengikuti Pelatihan ISO 27001:2022
      - Mempunyai pengalaman bekerja minimal 1 tahun
      - Mampu membuat dan mengimplementasikan prosedur kerja

b. Tugas dan wewenang

- **Tugas :**
  1. Melaksanakan dan mengawasi penerapan Kebijakan dan Standar SMKI di PT BPR BATU ARTOREJO pada bagian masing−masing;
  2. Memberi masukan untuk meningkatkan penerapan Kebijakan dan Standar SMKI kepada Ketua Tim Keamanan Informasi;
  3. Mendefinisikan kebutuhan dan merekomendasikan penyelenggaraan pelatihan keamanan informasi bagi personil PT BPR BATU ARTOREJO
  4. Memantau, mencatat, menguraikan, dan menindaklanjuti gangguan keamanan informasi yang diketahui atau dilaporkan sesuai prosedur pelaporan gangguan keamanan informasi pada Bagian masing−masing; dan
  5. Memberikan panduan dan atau bantuan penyelesaian masalah−masalah keamanan informasi pada Bagian masing−masing.
- **Wewenang :**
  Memiliki Akses terhadap Dokumen SMKI secara menyeluruh

3. INTERNAL AUDITOR

a. Syarat Kompetensi

- Min. Pendidikan SMA/SMK
- Pelatihan ISO 27001:2022
- Pelatihan ISO 19011:2018
- Menjabat sebagai Pejabat Eksekutif Internal Audit minimal selama 1 tahun
- Mampu membuat dan mengimplementasikan prosedur kerja
- Memiliki skill komunikasi yang baik
- Memiliki kemampuan Analisa yang baik

b. Tugas dan wewenang

- **Tugas :**
  1. Menyusun Program dan Jadwal Audit Internal SMKI,
  2. Melaksanakan Audit Internal SMKI,
  3. Melaporkan hasil Audit Internal SMKI kepada Pimpinan unit kerjanya,
  4. Mengevaluasi efektivitas pelaksanaan Audit Internal SMKI beserta kinerja Auditor,
  5. Mengusulkan kebutuhan peningkatan kompetensi auditor
- **Wewenang :**
  Memiliki Akses terhadap Dokumen SMKI secara menyeluruh

LAMPIRAN TIM SISTEM MANAJEMEN KEAMANAN INFORMASI PT BPR BATU ARTOREJO

JABATAN	NAMA PERSONIL	EVALUASI KESESUAIAN KOMPETENSI	KESESUAIAN	EVALUATOR	REKOMENDASI KOMPETENSI
Ketua Tim	WAHYUDIN	- Ijazah Min SMA/SMK - Sertifikat Awareness ISO 27001:2022 - Pelatihan Awareness ISO 19011:2018 - Memenuhi pengalaman kerja	Sesuai	Direksi	-
Anggota	PUSPITA RATNASARI	- Ijazah Min SMA/SMK - Sertifikat Awareness ISO 27001:2022 - Memenuhi pengalaman kerja	Sesuai	Direksi	-
Anggota	RUNIKA FITROH YUNIARTI	- Ijazah Min SMA/SMK - Sertifikat Awareness ISO 27001:2022 - Memenuhi pengalaman kerja	Sesuai	Direksi	-
Internal Audit	DWI ASTUTIK	- Ijazah D-III - Sertifikat Awareness ISO 27001:2022 - Sertifikat Awareness ISO 19011:2018 - Memenuhi pengalaman kerja	Sesuai	Direksi	-

Jakarta, 10 Agustus 2023
PT BPR BATU ARTOREJO

Ichwanul Ridwan SE., Ak
DIREKTUR

PT BANK PERKREDITAN RAKYAT
BATU ARTOREJO

KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI
PT. BPR BATU ARTOREJO

PT. BPR BATU ARTOREJO berkomitmen menerapkan Sistem Manajemen Keamanan Informasi berdasarkan ISO 27001:2022 dan senantiasa mematuhi peraturan perundang-undangan terkait pengamanan informasi yang berlaku serta melakukan perbaikan secara berkelanjutan terhadap sistem manajemen keamanan informasi.

PT. BPR BATU ARTOREJO berkomitmen dalam:

1. memastikan Kerahasiaan, integritas dan ketersediaan informasi melalui kendali organisasi yang tersertifikasi standar Internasional Sistem Manajemen Keamanan Informasi ISO 27001:2022 .
2. Menjaga keamanan informasi, data dan dokumen pada lingkungan yang terkendali, aman, dan terlindungi dari akses, penggunaan, atau pengungkapan yang tidak sah.
3. Menjaga pengamanan administratif, teknis, dan fisik yang wajar untuk perlindungan terhadap akses, penggunaan, modifikasi, dan pengungkapan tidak sah atas data pribadi dalam kendali dan pengawasannya.

Batu, 05 Oktober 2023

PT. BPR BATU ARTOREJO

Ichwanul Ridwan SE., Ak.

DIREKTUR

LEMBAR KETIDAKSESUAIAN (TEMUAN) AUDIT INTERNAL SMKI PT. BPR BATU ARTOREJO TAHUN 2023

No. FR.05.00/SOP.05.00/PND.01.00/601786/VIII/2023

Tanggal Audit: 10 Agustus 2023

Acuan Audit : Standar ISO 27001:2022

Auditor : Dwi Astutik

NO.	KLAUSUL/ REFERENSI	PIC	STATUS TEMUAN	KESESUAIAN/ KETIDAKSESUAIAN	KOREKSI	PENYEBAB KETIDAKSESUAIAN	TINDAKAN KOREKTIF DAN PENCEGAHAN	BUKTI DOKUMEN	VERIFIKASI AUDITOR
1									
2									
3									
4									
5									
6									

Dibuat oleh,

Dwi Astutik
Internal Auditor

Disetujui oleh,

Ichwanul Ridwan., SE., Ak.
Direktur

	Audit Prosedur & Checklist ISO 27001:2022	Indeks : - Bab : -
		SOP No : - Tanggal : 10 Agustus 2023 Revisi : 1 (satu)

Tingkat Kemungkinan

ISO 27001 Annex no	ISO 27001 Controls	Brief Description	Audit methods	Expected Evidences	Audit Results	Keterangan	Pelaksana & Tanggal	Reviewer & Tanggal
A.5	**Kontrol organisasi**							
A.5.1	kebijakan (Policy) untuk keamanan informasi	Juknis SMKI dan kebijakan (Policy) khusus topik harus didefinisikan, disetujui oleh manajemen, dipublikasikan, dikomunikasikan kepada dan diakui oleh personel yang relevan dan pihak yang berkepentingan terkait, dan ditinjau pada interval yang direncanakan dan jika perubahan signifikan terjadi.	Dapatkan SOP/Juknis SMKI, periksa isi ruang lingkup, tujuan, tanggal pengesahan & revisi kebijakan (Policy), otorisasi pejabat & bukti publikasi ke pihak terkait.	Dokumen kebijakan (Policy), SOP, Juknis keamanan informasi				
A.5.2	Peran dan tanggung jawab keamanan informasi	Peran dan tanggung jawab keamanan informasi harus didefinisikan dan dialokasikan sesuai dengan kebutuhan organisasi.	Periksa dokumen struktur organisasi information security & job description. Periksa apakah peran telah didefinisikan. Periksa apakah ada fungsi tumpang tindih dan/atau kerangkapan (rap)	- Dokumen struktur organisasi SMKI - Dokumen job description tim SMKI				
A.5.3	Pemisahan tugas	Tugas yang bertentangan dan bidang tanggung jawab yang saling bertentangan harus diatur.	Periksa dokumen struktur organisasi information security & job description. Periksa apakah peran telah didefinisikan. Periksa apakah ada fungsi tumpang tindih dan/atau	- Dokumen struktur organisasi SMKI - Dokumen job description tim SMKI				
A.5.4	Tanggung jawab manajemen	Manajemen harus mewajibkan semua personel untuk menerapkan keamanan informasi sesuai dengan Juknis SMKI yang ditetapkan, kebijakan (Policy) dan prosedur khusus untuk organisasi.	Periksa isi SOP/Juknis SMKI mencakup ruang lingkup & tanggung jawab karyawan/vendor serta penegakan. Periksa apakah karyawan/vendor sudah memahami kebijakan (Policy)/peraturan keamanan.	- Dokumen SOP/Juknis SMKI - Bukti sosialisasi SOP/Juknis SMKI (email, daftar hadir, dll)				
A.5.5	Kontak dengan pihak berwenang	Organisasi harus menjalin dan memelihara kontak dengan otor	Periksa apakah tim information security mengetahui nomor kontak dengan pihak berwenang, seperti Nomor kontak Tim SMKI Perbarindo, dll	Nomor kontak Tim SMKI Perbarindo				
A.5.6	Kontak dengan kelompok minat khusus	Organisasi harus menjalin dan memelihara kontak dengan kelompok kepentingan khusus atau forum keamanan spesialis lainnya dan asosiasi profesional.	Periksa apakah tim information security sudah tergabung dengan kelompok atau forum information security, seperti hackernews, dll	Email atau forum kelompok information security.				
A.5.7	Inteligensi ancaman	Informasi yang berkaitan dengan ancaman keamanan informasi harus dikumpulkan dan dianalisis untuk menghasilkan intelijen ancaman.	Periksa apakah terdapat informasi threat intelegence terkini dari forum, dll	Email atau forum kelompok information security.				
A.5.8	Keamanan informasi dalam manajemen proyek	Keamanan informasi harus diintegrasikan ke dalam manajeme	Periksa apakah ketentuan information security sudah termasuk dalam tahapan pengembangan atau proyek IT (aplikasi & infrastruktur).	- Dokumen SOP/Juknis SMKI - Dokumen SOP Project Management. - Sample Project Charter				
A.5.9	Inventarisasi informasi dan aset terkait lainnya	Inventarisasi informasi dan aset terkait lainnya, termasuk pemilik, harus dikembangkan dan dipelihara.	Dapatkan SOP/Juknis SMKI yang berkaitan dengan aset informasi & IT. Dapatkan daftar aset informasi & IT. Periksa apakah update & sudah ditentukan PIC pemilik/pengelola aset.	- Dokumen SOP Aset Manajemen. - Dokumen SOP/Juknis SMKI - Daftar aset informasi & IT.				
A.5.10	Penggunaan informasi dan aset terkait lainnya yang dapat diterima	Aturan untuk penggunaan dan prosedur yang dapat diterima untuk menangani informasi dan aset terkait lainnya harus diidentifikasi, didokumentasikan, dan dilaksanakan.	Dapatkan SOP/Juknis SMKI yang berkaitan dengan aset informasi & IT. Periksa apakah kebijakan (Policy) berisi aturan penggunaan aset informasi & IT. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI				
A.5.11	Pengembalian aset	Personil dan pihak berkepentingan lainnya sebagaimana mestinya harus mengembalikan semua aset organisasi yang mereka miliki setelah perubahan atau pemutusan hubungan kerja, kontrak atau perjanjian mereka.	Dapatkan SOP/Juknis SMKI yang berkaitan dengan aset informasi & IT. Periksa apakah kebijakan (Policy) berisi aturan pengembalian aset informasi & IT. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	#NAME?				
A.5.12	Klasifikasi informasi	Informasi harus diklasifikasikan menurut kebutuhan keamanan informasi organisasi berdasarkan kerahasiaan, integritas, ketersediaan, dan persyaratan pihak yang berkepentingan yang relevan.	Dapatkan SOP/Juknis SMKI yang berkaitan dengan aset informasi & IT. Periksa apakah kebijakan (Policy) berisi klasifikasi aset informasi & IT. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Daftar aset informasi				
A.5.13	Pelabelan informasi	Seperangkat prosedur yang tepat untuk pelabelan informasi harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.	Dapatkan SOP/Juknis SMKI yang berkaitan dengan aset informasi & IT. Periksa apakah kebijakan (Policy) berisi pelabelan aset informasi & IT. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Bukti pelabelan dokumen rahasia (elektronik & hardcopy)				
A.5.14	Transfer informasi	Aturan, prosedur, atau perjanjian transfer informasi harus ada untuk semua jenis fasilitas transfer dalam organisasi dan antara organisasi dan pihak lain.	Dapatkan SOP yang berkaitan dengan pengiriman data. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan data saat dikirim. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Fasilitas pengamanan data, seperti password, enkripsi, dll.				
A.5.15	Kontrol akses	Aturan untuk akses fisik dan logis ke informasi dan aset terkait lainnya harus ditetapkan dan diterapkan berdasarkan persyaratan keamanan bisnis dan informasi.	Dapatkan SOP/Juknis SMKI yang berkaitan akses pengguna & password. Periksa apakah kebijakan (Policy) berisi ketentuan permintaan, perubahan & penutupan akses. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- User Access Matrix - Dokumen SOP/Juknis SMKI				

A.5.16	Manajemen identitas	Siklus hidup penuh identitas harus dikelola.	Dapatkan SOP/Juknis SMKI yang berkaitan akses pengguna & password. Periksa apakah kebijakan (Policy) berisi ketentuan permintaan, perubahan & penutupan akses. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- User Access Matrix - Dokumen SOP/Juknis SMKI - Dokumen review user - Sample user baru - Sample penutupan user				
A.5.17	Informasi autentikasi	Alokasi dan pengelolaan informasi otentikasi harus dikendalikan oleh proses manajemen, termasuk memberi nasihat kepada personel tentang penanganan informasi otentikasi yang tepat.	Dapatkan SOP/Juknis SMKI yang berkaitan akses pengguna & password. Periksa apakah kebijakan (Policy) berisi ketentuan permintaan, perubahan & penutupan akses. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Dokumen/Berita Acara Penerimaan Password. - Sample User baru - Sample penutupan User				
A.5.18	Hak akses	Hak akses ke informasi dan aset terkait lainnya harus disediakan, ditinjau, dimodifikasi, dan dihapus sesuai dengan kebijakan (Policy) khusus topik organisasi tentang dan aturan untuk kontrol akses.	Dapatkan SOP/Juknis SMKI yang berkaitan akses pengguna & password. Periksa apakah kebijakan (Policy) berisi ketentuan permintaan, perubahan & penutupan akses. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Dokumen review User - Sample User baru - Sample penutupan User				
A.5.19	Keamanan informasi dalam hubungan pemasok	Proses dan prosedur harus didefinisikan dan diterapkan untuk mengelola risiko keamanan informasi yang terkait dengan penggunaan produk atau layanan pemasok.	Dapatkan SOP yang berkaitan dengan pengelolaan jasa pihak ketiga. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan yang harus dilakukan vendor. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen Juknis SMKI dengan vendor - Daftar vendor - PKS & NDA				
A.5.20	Menangani keamanan informasi dalam perjanjian pemasok	Persyaratan keamanan informasi yang relevan harus ditetapkan dan disetujui dengan masing-masing pemasok berdasarkan jenis hubungan pemasok.	Dapatkan SOP yang berkaitan dengan pengelolaan jasa pihak ketiga. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan yang harus dilakukan vendor. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen Juknis SMKI dengan vendor - Daftar vendor - PKS & NDA				
A.5.21	Mengelola keamanan informasi dalam rantai pasokan teknologi informasi dan komunikasi (TIK)	Risiko proses dan prosedur harus dikaitkan dengan produk TIK yang diterapkan untuk mengelola dan rantai pasokan layanan keamanan informasi.	Dapatkan SOP yang berkaitan dengan pengelolaan jasa pihak ketiga. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan yang harus dilakukan vendor. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen Juknis SMKI dengan vendor - Daftar vendor - PKS & NDA				
A.5.22	Pemantauan, peninjauan, dan manajemen perubahan layanan pemasok	Organisasi harus secara teratur memantau, meninjau, mengevaluasi, dan mengelola perubahan dalam praktik keamanan informasi pemasok dan pemberian layanan.	Dapatkan SOP yang berkaitan dengan pengelolaan jasa pihak ketiga. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan yang harus dilakukan vendor. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen Juknis SMKI dengan vendor - Daftar vendor - PKS & NDA				
A.5.23	Keamanan informasi untuk penggunaan layanan cloud	Proses untuk akuisisi, penggunaan, manajemen, dan keluar dari layanan cloud harus ditetapkan sesuai dengan persyaratan keamanan informasi organisasi.	Dapatkan SOP yang berkaitan dengan cloud computing dan pengelolaan jasa pihak ketiga. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan yang harus dilakukan vendor. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen Juknis SMKI dengan vendor - Daftar vendor - PKS & NDA - Daftar layanan cloud				
A.5.24	Perencanaan manajemen insiden keamanan informasi	Organisasi harus merencanakan dan mempersiapkan diri untuk mengelola insiden secu-rity informasi dengan mendefinisikan, membangun, dan mengkomunikasikan proses, peran, dan tanggung jawab manajemen insiden keamanan informasi.	Dapatkan SOP Security Insiden Manajemen. Periksa apakah kebijakan (Policy) tersebut berisi tahapan penanganan insiden & tim insiden. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Dokumen tim insiden keamanan. - Laporan atau berita acara insiden keamanan.				
A.5.25	Penilaian dan keputusan tentang acara keamanan dalam formasi	Organisasi harus menilai peristiwa keamanan informasi dan memutuskan apakah mereka akan dikategorikan sebagai insiden keamanan informasi.	Dapatkan SOP Security Insiden Manajemen. Periksa apakah kebijakan (Policy) tersebut berisi tahapan penanganan insiden & tim insiden. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Dokumen tim insiden keamanan. - Laporan atau berita acara insiden keamanan.				
A.5.26	Respons terhadap insiden keamanan informasi	Insiden keamanan informasi harus ditanggapi sesuai dengan prosedur yang didokumentasikan.	Dapatkan SOP Security Insiden Manajemen. Periksa apakah kebijakan (Policy) tersebut berisi tahapan penanganan insiden & tim insiden. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Dokumen tim insiden keamanan. - Laporan atau berita acara insiden keamanan.				
A.5.27	Belajar dari insiden keamanan informasi	Pengetahuan yang diperoleh dari insiden keamanan informasi harus digunakan untuk memperkuat dan meningkatkan kontrol keamanan informasi.	Dapatkan SOP Security Insiden Manajemen. Periksa apakah kebijakan (Policy) tersebut berisi tahapan penanganan insiden & tim insiden. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Dokumen tim insiden keamanan. - Laporan atau berita acara insiden keamanan.				
A.5.28	Pengumpulan bukti	Organisasi harus menetapkan dan menerapkan prosedur untuk identifikasi, pengumpulan, akuisisi, dan pelestarian bukti yang terkait dengan peristiwa keamanan informasi.	Dapatkan SOP Security Insiden Manajemen. Periksa apakah kebijakan (Policy) tersebut berisi tahapan penanganan insiden & tim insiden. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Dokumen tim insiden keamanan. - Laporan atau berita acara insiden keamanan.				
A.5.29	Keamanan informasi selama gangguan	Organisasi harus merencanakan bagaimana menjaga keamanan informasi pada tingkat yang sesuai selama gangguan.	Dapatkan kebijakan/SOP BCP & DRP. Periksa apakah kebijakan tersebut berisi tahapan & tim pemulihan aplikasi & bisnis jika terjadi bencana. Periksa implementasinya apakah telah sesuai	- Dokumen penanganan insiden - Laporan insiden / trouble - Dokumen Call Tree / Emergency Call				
A.5.30	Kesiapan TIK untuk kelangsungan bisnis	Kesiapan TIK harus direncanakan, dilaksanakan, dipelihara dan diuji berdasarkan tujuan kelangsungan bisnis dan persyaratan kontinuitas TIK.	Dapatkan kebijakan/SOP BCP & DRP. Periksa apakah kebijakan tersebut berisi tahapan & tim pemulihan aplikasi & bisnis jika terjadi bencana. Periksa implementasinya apakah telah sesuai	- Dokumen BCP/DRP				
A.5.31	Persyaratan hukum, undang-undang, peraturan, dan kontrak	Persyaratan hukum, undang-undang, peraturan, dan kontraktual yang relevan dengan keamanan informasi dan pendekatan organisasi untuk memenuhi persyaratan ini harus diidentifikasi, didokumentasikan, dan selalu diperbarui.	Dapatkan SOP evaluasi efektivitas implementasi standar keamanan. Periksa apakah terdapat persyaratan keamanan dari regulasi yang harus direview implementasinya secara rutin.	- Laporan bulanan SMKI - Laporan menajemen review ISO 27001.				

A.5.32	Hak kekayaan intelektual	Organisasi harus menerapkan prosedur yang tepat untuk melindungi hak kekayaan intelektual.	Dapatkan SOP/Juknis SMKI. Periksa apakah kebijakan (Policy) tersebut sudah melarang penggunaan aplikasi yang melanggar HAKI. Periksa implementasinya apakah telah sesuai dengan	- Dokumen SOP review keamanan informasi - Laporan review rutin keamanan informasi ISO 27001 - Daftar aset IT				
A.5.33	Perlindungan catatan	Catatan harus dilindungi dari kehilangan, penghancuran, pemalsuan, akses tidak sah, dan pelepasan yang tidak sah.	Dapatkan Juknis SMKI. Periksa apakah kebijakan tersebut berisi ketentuan perlindungan dokumen atau bukti-bukti pengamanan informasi. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Laporan bulanan SMKI - Laporan menajemen review ISO 27001.				
A.5.34	Privasi dan perlindungan informasi identitas pribadi (PII)	Organisasi harus mengidentifikasi dan memenuhi persyaratan mengenai pelestarian privasi dan perlindungan PII sesuai dengan undang-undang dan peraturan yang berlaku dan persyaratan kontrak.	Dapatkan SOP/Juknis SMKI. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan perlindungan dokumen atau data pribadi. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen Juknis SMKI				
A.5.35	Tinjauan independen keamanan informasi	Pendekatan organisasi untuk mengelola keamanan informasi dan implementasinya termasuk orang, proses, dan teknologi harus ditinjau secara independen pada interval yang direncanakan, atau ketika perubahan signifikan terjadi.	Dapatkan kebijakan/SOP yang berkaitan dengan audit IT. Periksa apakah kebijakan tersebut berisi ketentuan internal audit melakukan audit IT secara rutin. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen Juknis SMKI. - Laporan hasil audit SMKI.				
A.5.36	Kepatuhan terhadap kebijakan (Policy), aturan, dan standar untuk keamanan informasi	Kepatuhan terhadap Juknis SMKI organisasi, kebijakan (Policy), aturan, dan standar khusus topik harus ditinjau secara teratur.	Dapatkan kebijakan/SOP evaluasi efektivitas implementasi standar keamanan. Periksa apakah terdapat persyaratan keamanan dari regulasi yang harus direview implementasinya	- Juknis SMKI - Sosialisasi Juknis SMKI				
A.5.37	Prosedur operasi yang terdokumentasi	Prosedur operasi untuk fasilitas pemrosesan informasi harus didokumentasikan dan disediakan untuk personel yang membutuhkannya.	Dapatkan SOP Operasional IT, seperti backup, penanganan insiden, monitoring infrastruktur, dll. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Dokumen SOP JB				
A.6	**Kontrol Pegawai**							
A.6.1	Penyaringan	Pemeriksaan verifikasi latar belakang pada semua kandidat untuk menjadi personel harus dilakukan sebelum bergabung dengan organisasi dan secara berkelanjutan dengan mempertimbangkan hukum, peraturan, dan etika yang berlaku dan proporsional dengan persyaratan bisnis.	Periksa apakah sudah terdapat peraturan atau ketentuan keamanan berupa screening atau background check dalam proses rekruitmen atau karyawan sebelum dipekerjakan.	- Dokumen SOP/Juknis SMKI - Dokumen SOP Pelatihan, Rekruitmen, Mutasi & Berhenti Kerja dari SDI - Dokumen Bukti screening atau background check				
A.6.2	Syarat dan ketentuan kerja	Perjanjian kontrak kerja harus menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi.	Periksa apakah sudah terdapat kebijakan (Policy) keamanan dalam proses SDM. Periksa apakah karyawan/vendor menandatangani tanggung jawab dalam menajaga keamanan.	- Dokumen SOP/Juknis SMKI - Dokumen SOP Pelatihan, Rekruitmen, Mutasi & Berhenti Kerja dari SDI - Dokumen NDA atau perjanjian kerahasiaan yang ditandatangani karyawan/vendor.				
A.6.3	Kesadaran, pendidikan, dan pelatihan keamanan informasi	Orang yang berkepentingan dengan organ dan pihak-pihak yang berkepentingan terkait harus menerima kesadaran keamanan informasi yang sesuai, pendidikan dan pelatihan dan pembaruan rutin dari Juknis SMKI organisasi, kebijakan (Policy) dan prosedur khusus topik, yang relevan untuk fungsi pekerjaan mereka.	Dapatkan SOP/Juknis SMKI. Periksa apakah karyawan/vendor medapatkan pemahaan/sosialisasi secara rutin mengenai kebijakan (Policy)/peraturan keamanan.	- Dokumen SOP/Juknis SMKI - Dokumen SOP Pelatihan, Rekruitmen, Mutasi & Berhenti Kerja dari SDI - Bukti sosialisasi SOP/Juknis SMKI (email, daftar hadir, dll) - Bukti pelatihan keamanan informasi.				
A.6.4	Proses disipliner	Proses disipliner harus diformalkan dan dikomunikasikan untuk mengambil tindakan terhadap personel dan pihak berkepentingan terkait lainnya yang telah melakukan	Dapatkan SOP/Juknis SMKI. Periksa apakah terdapat sanksi pelanggaran jika tidak mematuhi SOP tsb.	- Dokumen SOP/Juknis SMKI - Dapatkan SOP/Juknis SMKI. Periksa apakah karyawan/vendor medapatkan pemahaan/sosialisasi				
A.6.5	Tanggung jawab setelah masa jabatan atau perubahan pekerjaan	Tanggung jawab dan tugas keamanan informasi yang tetap berlaku setelah pemutusan hubungan kerja atau perubahan pekerjaan harus didefinisikan, ditegakkan, dan dikomunikasikan kepada personel terkait dan pihak	Dapatkan SOP/Juknis SMKI. Periksa apakah terdapat sanksi pelanggaran jika tidak mematuhi SOP tsb.	- Exit Clearence - Dokumenkebijakan (Policy) mutasi, resign / pemutusan kerja				
A.6.6	Confidentiality or non-disclosure agreements	Perjanjian kerahasiaan atau kerahasiaan yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, didokumentasikan, ditinjau secara teratur dan ditandatangani oleh personel dan pihak berkepentingan terkait lainnya.	Dapatkan SOP yang berkaitan dengan menjaga kerahasiaan. Periksa apakah karyawan & vendor sudah menandatangani NDA dan paham mengenai aturan keamanan.. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Fasilitas pengamanan data, seperti password, enkripsi, dll. - Dokumen NDA karyawan & vendor.				
A.6.7	Kerja jarak jauh	Langkah-langkah keamanan harus diterapkan ketika personel bekerja dari jarak jauh untuk melindungi informasi yang diakses, diproses, atau disimpan di luar lokasi organisasi.	Periksa apakah sudah terdapat ketentuan atau peraturan keamanan untuk perangkat bergerak dan teleworking.	- Dokumen SOP/Juknis SMKI - Laporan Pemeriksaan VPN - Form pengajuan akses teleworking. - Daftar user VPN.				
A.6.8	Pelaporan peristiwa keamanan informasi	Organisasi harus menyediakan mekanisme bagi personel untuk melaporkan peristiwa keamanan informasi yang diamati atau dicurigai melalui saluran yang sesuai secara tepat waktu.	Dapatkan SOP penanganan insiden keamanan. Periksa apakah kebijakan (Policy) tersebut berisi tahapan penanganan insiden keamanan. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Dokumen tim insiden keamanan. - Laporan atau berita acara insiden keamanan.				
A.7	**Kontrol fisik**							
A.7.1	Perimeter keamanan fisik	Perimeter keamanan harus didefinisikan dan digunakan untuk melindungi area yang berisi informasi dan aset terkait lainnya.	Dapatkan SOP/Juknis SMKI yang berkaitan keamanan fisik ruangan dan data center/DRC. Periksa apakah kebijakan (Policy) berisi ketentuan pengamanan ruangan & lingkungan seperti CCTV, kunci elektronik, UPS, AC, alat pemadam kebakaran, smoke detector, dll. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Fasilitas pengamanan ruangan & lingkungan, seperti CCTV, UPS, AC. APAR, kunci elektronik, smoke detektor, dll.				
A.7.2	Entri fisik	Area aman harus dilindungi oleh kontrol masuk dan titik akses yang sesuai.	Dapatkan SOP/Juknis SMKI yang berkaitan keamanan fisik ruangan dan data center/DRC. Periksa apakah kebijakan (Policy) berisi ketentuan pengamanan ruangan & lingkungan seperti CCTV, kunci elektronik, UPS, AC, alat pemadam kebakaran, smoke detector, dll. Periksa implementasinya	- Dokumen SOP/Juknis SMKI - Fasilitas pengamanan ruangan & data center, seperti CCTV, UPS, AC. APAR, kunci elektronik, smoke detektor, dll - Daftar karyawan yang akses kantor				

A.7.3	Mengamankan kantor, ruangan, dan fasilitas	Keamanan fisik untuk kantor, ruangan dan fasilitas harus dirancang dan dilaksanakan.	Dapatkan SOP/Juknis SMKI yang berkaitan keamanan fisik ruangan dan data center/DRC. Periksa apakah kebijakan (Policy) berisi ketentuan pengamanan ruangan & lingkungan seperti CCTV, kunci elektronik, UPS, AC, alat pemadam kebakaran, smoke detector, dll. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Fasilitas pengamanan ruangan & data center, seperti CCTV, UPS, AC. APAR, kunci elektronik, smoke detektor, dll - Daftar karyawan yang akses kantor				
A.7.4	Pemantauan keamanan fisik	Tempat harus terus dipantau untuk akses fisik yang tidak sah.	Dapatkan SOP/Juknis SMKI yang berkaitan keamanan fisik ruangan dan data center/DRC. Periksa apakah kebijakan (Policy) berisi ketentuan pengamanan ruangan & lingkungan seperti CCTV, kunci elektronik, UPS, AC, alat pemadam kebakaran, smoke detector, dll. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Fasilitas pengamanan ruangan & lingkungan, seperti CCTV, UPS, AC. APAR, kunci elektronik, smoke detektor, dl - Dokumen Review akses fisik / entry fisik				
A.7.5	Melindungi dari ancaman fisik dan lingkungan	Perlindungan terhadap ancaman fisik dan lingkungan, seperti bencana alam dan ancaman fisik yang disengaja atau tidak disengaja lainnya terhadap infrastruktur harus dirancang dan dilaksanakan.	Dapatkan SOP/Juknis SMKI yang berkaitan keamanan fisik ruangan dan data center/DRC. Periksa apakah kebijakan (Policy) berisi ketentuan pengamanan ruangan & lingkungan seperti CCTV, kunci elektronik, UPS, AC, alat pemadam kebakaran, smoke detector, dll. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Fasilitas pengamanan ruangan & lingkungan, seperti CCTV, UPS, AC. APAR, kunci elektronik, smoke detektor, dl - Dokumen Review akses fisik / entry fisik				
A.7.6	Clear desk and clear	Langkah-langkah keamanan untuk bekerja di area yang aman harus dirancang dan diimplementasikan.	Dapatkan SOP/Juknis SMKI yang berkaitan keamanan fisik ruangan dan data center/DRC. Periksa apakah kebijakan (Policy) berisi ketentuan pengamanan ruangan & lingkungan seperti CCTV, kunci elektronik, UPS, AC, alat pemadam kebakaran, smoke detector, dll. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Fasilitas pengamanan ruangan & data center, seperti CCTV, UPS, AC. APAR, kunci elektronik, smoke detektor, dll - Daftar karyawan yang akses kantor				
A.7.7	Clear desk and clear screen	Aturan meja yang jelas untuk kertas dan media penyimpanan yang dapat dilepas dan aturan layar yang jelas untuk fasilitas pemrosesan informasi harus didefinisikan dan ditegakkan dengan tepat.	Dapatkan SOP/Juknis SMKI yang berkaitan clean desk & clear screen. Periksa apakah kebijakan (Policy) berisi ketentuan pengguna screen saver & pengamanan dokumen rahasi di meja/ruangan. Periksa implementasinya apakah telah sesuai	- Dokumen SOP/Juknis SMKI - Fasilitas pengamanan screen saver, lemari penyimpanan dokumen/data rahasia.				
A.7.8	Equipment siting and protection	Peralatan harus ditempatkan dengan aman dan terlindungi.						
A.7.9	Keamanan aset di luar lokasi	Aset di luar lokasi harus dilindungi.	Dapatkan SOP/Juknis SMKI yang berkaitan keamanan fisik ruangan dan data center/DRC. Periksa apakah kebijakan (Policy) berisi ketentuan pengamanan ruangan & lingkungan seperti CCTV, kunci elektronik, UPS, AC, alat pemadam kebakaran, smoke detector, dll. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Fasilitas pengamanan ruangan & lingkungan, seperti CCTV, UPS, AC. APAR, kunci elektronik, smoke detektor, dl				
A.7.10	Media penyimpanan	Media penyimpanan harus dikelola melalui siklus hidup akuisisi, penggunaan, transportasi, dan pembuangannya sesuai dengan skema klasifikasi organisasi dan persyaratan	Dapatkan SOP/Juknis SMKI yang berkaitan keamanan fisik ruangan dan data center/DRC. Periksa apakah kebijakan (Policy) berisi ketentuan pengamanan ruangan & lingkungan	- Dokumen Juknis SMKI - Berita acara pengiriman tape backup / media penyimpanan				
A.7.11	Utilitas pendukung	Fasilitas pemrosesan informasi harus dilindungi dari kegagalan daya dan gangguan lain yang disebabkan oleh kegagalan dalam mendukung utilitas.	Dapatkan SOP/Juknis SMKI yang berkaitan keamanan fisik ruangan dan data center/DRC. Periksa apakah kebijakan (Policy) berisi ketentuan pengamanan ruangan & lingkungan seperti CCTV, kunci elektronik, UPS, AC, alat pemadam kebakaran, smoke detector, dll. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Fasilitas pengamanan ruangan & lingkungan, seperti CCTV, UPS, AC. APAR, kunci elektronik, smoke detektor, dl				
A.7.12	Keamanan kabel	Kabel yang membawa daya, data, atau layanan informasi pendukung harus dilindungi dari intersepsi, gangguan, atau kerusakan.	Dapatkan SOP/Juknis SMKI yang berkaitan keamanan fisik ruangan dan data center/DRC. Periksa apakah kebijakan (Policy) berisi ketentuan pengamanan ruangan & lingkungan seperti CCTV, kunci elektronik, UPS, AC, alat pemadam kebakaran, smoke detector, dll. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Fasilitas pengamanan ruangan & lingkungan, seperti CCTV, UPS, AC. APAR, kunci elektronik, smoke detektor, dl				
A.7.13	Perawatan peralatan	Peralatan harus dijaga dengan benar untuk memastikan ketersediaan, integritas, dan kerahasiaan informasi.	Dapatkan SOP/Juknis SMKI yang berkaitan keamanan fisik ruangan dan data center/DRC. Periksa apakah kebijakan (Policy) berisi ketentuan pengamanan ruangan & lingkungan seperti CCTV, kunci elektronik, UPS, AC, alat pemadam kebakaran, smoke detector, dll. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Fasilitas pengamanan ruangan & lingkungan, seperti CCTV, UPS, AC. APAR, kunci elektronik, smoke detektor, dl - Maintenance Peralatan				
A.7.14	Pembuangan atau penggunaan kembali peralatan yang aman	Item peralatan yang mengandung media penyimpanan harus diverifikasi untuk memastikan bahwa setiap data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa dengan aman sebelum dibuang atau digunakan kembali.	Dapatkan SOP/Juknis SMKI yang berkaitan penghancuran/penghapusan informasi atau aset IT. Periksa apakah kebijakan (Policy) berisi ketentuan penghapusan data & aset IT secara aman. Periksa implementasinya apakah telah	- Dokumen SOP/Juknis SMKI - Berita Acara penghapusan data atau aset IT. - Fasilitas penghapusan data/aset IT, seperti shredder atau tool penghapusan sesuai DoD-5502				
A.8	**Kontrol teknologi**							
A.8.1	Perangkat titik akhir pengguna	Informasi yang disimpan pada, diproses oleh, atau dapat diakses melalui perangkat titik akhir pengguna harus dilindungi.	Dapatkan SOP/Juknis SMKI yang berkaitan akses pengguna. Periksa apakah kebijakan (Policy) berisi ketentuan permintaan, perubahan & penutupan akses. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Daftar user yang bisa akses aplikasi JB - Antivirus.				
A.8.2	Hak akses istimewa	Alokasi dan penggunaan hak akses istimewa harus dibatasi dan dikelola.	Dapatkan SOP/Juknis SMKI yang berkaitan akses pengguna. Periksa apakah kebijakan (Policy) berisi ketentuan permintaan, perubahan & penutupan akses. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Daftar user yang bisa akses aplikasi JB - Antivirus.				
A.8.3	Pembatasan akses informasi	Akses ke informasi dan aset terkait lainnya harus dibatasi sesuai dengan kebijakan (Policy) khusus topik yang ditetapkan tentang kontrol akses.	Dapatkan SOP/Juknis SMKI yang berkaitan akses pengguna & password. Periksa apakah kebijakan (Policy) berisi ketentuan permintaan, perubahan & penutupan akses. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Dokumen user akses matriks. - Dokumen berita acara review user akses				
A.8.4	Akses ke kode sumber	Akses baca dan tulis ke kode sumber, alat pengembangan, dan pustaka perangkat lunak harus dikelola dengan tepat.	Dapatkan SOP/Juknis SMKI yang berkaitan akses pengguna & password. Periksa apakah kebijakan (Policy) berisi ketentuan permintaan, perubahan & penutupan akses. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Dokumen user akses ke source code.				

A.8.5	Autentikasi aman	Teknologi dan prosedur otentikasi yang aman harus diterapkan berdasarkan pembatasan akses informasi dan kebijakan (Policy) khusus topik tentang kontrol akses.	Dapatkan SOP/Juknis SMKI yang berkaitan akses pengguna & password. Periksa apakah kebijakan (Policy) berisi ketentuan permintaan, perubahan & penutupan akses. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Dokumen form pengajuan akses & tanda tangan pemohon untuk menjaga akses. - Setting password pada aplikasi & infrastruktur IT.				
A.8.6	Manajemen kapasitas	Penggunaan sumber daya harus dipantau dan disesuaikan sesuai dengan kebutuhan kapasitas saat ini dan yang diharapkan.	Dapatkan SOP Operasional IT, seperti backup, penanganan insiden, monitoring infrastruktur, dll. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Dokumen SOP Operasional JB - Dokumen rencana kapasitas dan penggunaan kapasitas				
A.8.7	Perlindungan terhadap malware	Perlindungan terhadap malware harus diterapkan dan didukung oleh kesadaran pengguna yang sesuai.	Dapatkan SOP antimalware. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan implementasi antiwalre pada PC, laptop & server (jika OS Windows). Periksa implementasinya	- Dokumen SOP pengembangan aplikasi - Fasilitas antimalware . - Fasilitas antimalware yg update pada PC & laptop.				
A.8.8	Manajemen kerentanan teknis	Informasi tentang kerentanan teknis sistem informasi yang digunakan harus diperoleh, paparan organisasi terhadap kerentanan tersebut harus dievaluasi dan tindakan yang	Dapatkan SOP yang berkaitan dengan pengujian rutin kelemahan keamanan (vulnerability assessment & penetration test). Periksa implementasinya apakah telah sesuai dengan	- Dokumen SOP/Juknis SMKI. - Laporan vulnerability assessment dan penetration test secara rutin				
A.8.9	Manajemen konfigurasi	Konfigurasi, termasuk konfigurasi keamanan, perangkat keras, perangkat lunak, layanan, dan jaringan harus dibuat, didokumentasikan, diimplementasikan, dipantau, dan ditinjau.	Dapatkan SOP Operasional IT, seperti backup, penanganan insiden, monitoring infrastruktur, dll. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Juknis SMKI - Parameter setting OS Windows & JB				
A.8.10	Penghapusan informasi	Informasi yang disimpan dalam sistem informasi, perangkat atau di media penyimpanan lainnya harus dihapus ketika tidak lagi diperlukan.	Dapatkan SOP/Juknis SMKI yang berkaitan akses pengguna & password. Periksa apakah kebijakan (Policy) berisi ketentuan permintaan, perubahan & penutupan akses. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Dokumen disposal				
A.8.11	Masking data	Masking data harus digunakan sesuai dengan kebijakan (Policy) khusus topik organisasi tentang akses dan kebijakan (Policy) khusus topik terkait lainnya, dan persyaratan bisnis, dengan mempertimbangkan undang-undang yang berlaku.	Dapatkan SOP/Juknis SMKI yang berkaitan dengan aset informasi & IT. Periksa apakah kebijakan (Policy) berisi ketentuan masking data.	- Dokumen SOP/Juknis SMKI - Daftar aset informasi				
A.8.12	Pencegahan kebocoran data	Tindakan pencegahan kebocoran data harus diterapkan pada sistem, jaringan, dan perangkat lain yang memproses, menyimpan, atau mengirimkan informasi sensitif.	Dapatkan SOP/Juknis SMKI yang berkaitan dengan aset informasi & IT. Periksa apakah kebijakan (Policy) berisi pencegahan kebocoran data	- Dokumen SOP/Juknis SMKI - Daftar aset informasi				
A.8.13	Cadangan informasi	Salinan cadangan informasi, perangkat lunak, dan sistem harus dipelihara dan diuji secara teratur sesuai dengan kebijakan (Policy) khusus topik yang disepakati tentang pencadangan.	Dapatkan SOP backup dan BCP/DRP. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan backup secara rutin data rahasia & kritikal. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP backup. - Dokumen BCP & DRP. - Fasilitas & data backup yang update.				
A.8.14	Redundansi fasilitas pemrosesan informasi	Fasilitas pemrosesan informasi harus dilaksanakan dengan redundansi yang cukup untuk memenuhi persyaratan	Dapatkan SOP backup dan BCP/DRP. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan backup secara rutin data	- Daftar asset hardware data center dan DRC				
A.8.15	Logging	Log yang merekam aktivitas, pengecualian, kesalahan, dan peristiwa relevan lainnya harus diproduksi, disimpan, dilindungi, dan dianalisis.	Dapatkan SOP yang berkaitan dengan log pada PC, laptop, server dan aplikasi. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan aktivasi log. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Fasilitas log pada pada PC, laptop, server, aplikasi.				
A.8.16	Kegiatan pemantauan	Jaringan, sistem, dan aplikasi harus dipantau untuk perilaku anomali dan tindakan yang tepat yang diambil untuk mengevaluasi potensi insiden keamanan informasi.	Dapatkan SOP/Juknis SMKI. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pemantauan keamanan. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Lapran server dan lainnya/ laporan bulanan. - Laporan SoC.				
A.8.17	Sinkronisasi waktu	Jam sistem pemrosesan informasi yang digunakan oleh organisasi harus disinkronkan ke sumber waktu yang disetujui.	Dapatkan SOP yang berkaitan dengan log pada PC, laptop, server dan aplikasi. Periksa apakah kebijakan (Policy) tersebut berisi seluruh sistem harus menggunakan acuan waktu yang sama (sinkronisasi). Periksa implementasinya apakah telah	- Dokumen SOP/Juknis SMKI. - Fasilitas waktu yang tercatat pada PC, laptop, server, aplikasi sudah sinkron.				
A.8.18	Penggunaan program utilitas istimewa	Penggunaan program utilitas yang dapat menggantikan kontrol sistem dan aplikasi harus dibatasi dan dikontrol dengan ketat.	Dapatkan SOP/Juknis SMKI yang berkaitan akses pengguna & password. Periksa apakah kebijakan (Policy) berisi ketentuan permintaan, perubahan & penutupan akses. Periksa	- Dokumen SOP/Juknis SMKI - Daftar standar tool yang dipakai. - User yang bisa mengakses tools.				
A.8.19	Instalasi perangkat lunak pada sistem operasional	Prosedur dan langkah-langkah harus diterapkan untuk mengelola instalasi perangkat lunak dengan aman pada sistem operasional.	Dapatkan SOP yang berkaitan dengan akses. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan akses instalasi perangkat lunak hanya diberikan secara terbatas. Ke orang yang berwenang. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Daftar standar perangkat lunak. - Form Permintaan Instalasi Aplikasi/Software Khusus - Daftar user akses dan level akses di server, PC & laptop.				
A.8.2	Keamanan jaringan	Jaringan dan perangkat jaringan harus diamankan, dikelola, dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi.	Dapatkan SOP yang berkaitan dengan keamanan jaringan. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan jaringan. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Daftar Segmentasi jaringan. - Daftar user yang bisa akses ke jaringan internal & wifi.				
A.8.21	Keamanan layanan jaringan	Mekanisme keamanan s, tingkat layanan dan persyaratan layanan layanan jaringan harus diidentifikasi, diimplementasikan dan dipantau.	Dapatkan SOP yang berkaitan dengan keamanan jaringan. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan jaringan. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Daftar Segmentasi jaringan. - Daftar user yang bisa akses ke jaringan internal & wifi.				
A.8.22	Pemisahan jaringan	Kelompok layanan informasi, pengguna, dan sistem informasi harus dipisahkan dalam jaringan organisasi.	Dapatkan SOP yang berkaitan dengan keamanan jaringan. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan jaringan. Periksa implementasinya apakah telah	- Dokumen SOP/Juknis SMKI. - Pemisahan jaringan internal dan publik				
A.8.23	Pemfilteran web	Akses ke situs web eksternal harus dikelola untuk mengurangi paparan konten berbahaya.	Dapatkan SOP/Juknis SMKI. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan perlindungan enkripsi. Periksa	- Dokumen antivirus/firewall				
A.8.24	Penggunaan kriptografi	Aturan untuk penggunaan kriptografi yang efektif, termasuk manajemen kunci kriptografi, harus didefinisikan dan diimplementasikan.	Dapatkan SOP/Juknis SMKI. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan perlindungan enkripsi. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI - Daftar enkripsi yang dipakai. - User yang bisa mengakses file dan folder penyimpanan enkripsi di server				
A.8.25	Siklus hidup pengembangan yang aman	Aturan untuk pengembangan perangkat lunak dan sistem yang aman harus ditetapkan dan diterapkan.	Dapatkan SOP yang berkaitan dengan pengembangan aplikasi. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan aplikasi saat di develop. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Dokumen SOP Pengembangan Aplikasi. - Dokumen desgin (FSD) aplikasi berisi security control sesuai ketentuan. - Laporan hasil UAT & Security Test aplikasi				
A.8.26	Persyaratan keamanan aplikasi	Persyaratan keamanan informasi harus diidentifikasi, ditentukan, dan disetujui saat mengembangkan atau memperoleh aplikasi	Dapatkan SOP yang berkaitan dengan pengembangan aplikasi. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan aplikasi saat di develop. Periksa implementasinya	- Dokumen SOP/Juknis SMKI. - Dokumen SOP Pengembangan Aplikasi. - Dokumen desgin (FSD) aplikasi berisi security control				

A.8.27	Arsitektur sistem dan prinsip-prinsip rekayasa yang aman	Prinsip-prinsip untuk rekayasa sistem yang aman harus ditetapkan, didokumentasikan, dipelihara dan diterapkan pada setiap kegiatan pengembangan sistem informasi.	Dapatkan SOP yang berkaitan dengan pengembangan aplikasi. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan aplikasi saat di develop. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Dokumen SOP Pengembangan Aplikasi. - Dokumen desgin (FSD) aplikasi berisi security control sesuai ketentuan. - Laporan hasil UAT & Security Test aplikasi.				
A.8.28	Pengkodean aman	Prinsip pengkodean yang aman harus diterapkan pada pengembangan perangkat lunak.	Dapatkan SOP/Juknis SMKI. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan secure coding. Periksa	- Dokumen SOP/Juknis SMKI. - Dokumen SOP Pengembangan Aplikasi.				
A.8.29	Pengujian keamanan dalam pengembangan dan penerimaan	Proses pengujian keamanan harus didefinisikan dan diimplementasikan dalam siklus hidup pengembangan.	Dapatkan SOP yang berkaitan dengan pengembangan aplikasi. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan aplikasi saat di develop. Periksa implementasinya	- Dokumen SOP/Juknis SMKI. - Laporan hasil UAT & security test aplikasi.				
A.8.30	Pengembangan outsourcing	Organisasi harus mengarahkan, memantau dan meninjau kegiatan yang terkait dengan pengembangan sistem outsourcing.	Dapatkan SOP yang berkaitan dengan pengembangan aplikasi. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan aplikasi saat di develop. Periksa implementasinya	- Dokumen SOP/Juknis SMKI. - NDA perusahaan & personil pengembang pihak ketiga.				
A.8.31	Perlindungan informasi systems selama pengujian audit	Lingkungan pengembangan, pengujian, dan produksi harus dipisahkan dan diamankan.	Dapatkan SOP/Juknis SMKI. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan perlindungan dokumen atau data pribadi. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Laporan hasil audit				
A.8.32	Manajemen perubahan	Perubahan pada fasilitas pemrosesan informasi dan sistem informasi harus tunduk pada perubahan prosedur manajemen.	Dapatkan SOP manajemen perubahan aplikasi dan infrastruktur IT. Periksa apakah kebijakan (Policy) tersebut berisi prosedur & form pengajuan perubahan. Periksa	- Dokumen SOP Manajemen Perubahan. - Dokumen form pengajuan perubahan aplikasi atau infrastruktur IT.				
A.8.33	Menguji informasi	Informasi pengujian harus dipilih, dilindungi, dan dikelola dengan tepat.	Dapatkan SOP yang berkaitan dengan pengembangan aplikasi. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan pengamanan aplikasi saat di develop. Periksa implementasinya apakah telah sesuai dengan ketentuan tsb.	- Dokumen SOP/Juknis SMKI. - Dokumen SOP Penggunaan Data Uji.				
A.8.34	Perlindungan informasi systems selama pengujian audit	Tes audit dan kegiatan jaminan lainnya yang melibatkan penilaian sistem operasional harus direncanakan dan disepakati antara penguji dan manajemen yang sesuai.	Dapatkan SOP/Juknis SMKI. Periksa apakah kebijakan (Policy) tersebut berisi ketentuan perlindungan dokumen atau data pribadi. Periksa implementasinya apakah telah sesuai dengan	- Laporan hasil audit				

Laporan Tinjuan Manajemen ISO 27001 SMKI PT BPR BATU ARTOREJO

Semester 2 (Q3 - Q4) Tahun 2023

Tim SMKI - PT BPR BATU ARTOREJO

Document Control	
Judul Dokumen	Manajemen Review ISO 27001 SMKI Semester 2 2023
No Document	FR.01.00/PND.01.00/PERB-SMKI/XI/2023
Versi Dokumen	-
Tanggal	

Dibuat oleh	Direview dan disetujui oleh:
	
PUSPITA RATNASARI	Wahyudin
Tim SMKI	Ketua SMKI

Daftar Isi

1. Pendahuluan

Latar Belakang & Tujuan

Salah satu wujud komitmen manajemen PT BPR BATU ARTOREJO menjaga keamanan informasi perusahaan adalah menerapkan ISO 27001:2022 Sistem Manajemen Keamanan Informasi (SMKI) dan melaksanakan review secara berkala.

Tujuan dari laporan Manajemen Review (MR) ini adalah:

- Untuk memastikan tujuan & sasaran SMKI tercapai.
- Untuk memastikan kesesuaian, kecukupan dan efektivitas pelaksanaan SMKI.
- Untuk melakukan perbaikan terhadap implementasi SMKI secara berkelanjutan.
- Untuk mengidentifikasi perubahan eksternal dan internal yang berdampak terhadap SMKI serta mengambil keputusan yang tepat dalam merespon perubahan tersebut.

Tim SMKI menyiapkan rencana Manajemen Review secara keseluruhan sesuai persyaratan standar ISO 27001 dan kebutuhan PT BPR BATU ARTOREJO

Prosedur Manajemen Review telah menjadwalkan tiap semester.

Prosedur Manajemen Review juga telah menetapkan agenda pembahasan Manajemen Review, yaitu:

a) Status tindakan dari reviu manajemen sebelumnya;.
b) Perubahan isu eksternal dan internal yang relevan dengan SMKI.
c) Umpan balik dari pihak yang berkepentingan;
d) Hasil penilaian risiko dan status rencana penanganan risiko.
e) Peluang untuk perbaikan berkelanjutan.
f) Umpan balik dari kinerja keamanan informasi, termasuk kecenderungan dalam hal:
    - ketidaksesuaian dan tindakan korektif;
    - hasil pemantauan dan pengukuran;
    - hasil audit; dan
    - pemenuhan terhadap sasaran keamanan informasi.

2. Status Management Review Sebelumnya

Tidak terdapat Management Review selama bulan Januari – Juni 2023. Sesuai Rencana SMKI Tahun 2023 bahwa Manajemen Review akan dilakukan sebanyak 2 (dua) kali, yaitu pada Juli & Desember 2023.

No.	Permasalahan	Status	Arahan Ketua SMKI
1.	-		

3. Perubahan Isu Eksternal dan Internal

Selama periode Semester II 2023 tidak terdapat perubahan isu internal & eksternal yang mempengaruhi SMKI PT BPR BATU ARTOREJO.

Perubahan Isu Eksternal dan Internal Semester II 2023:

No.	Perubahan	Dampak	Arahan Ketua SMKI
1.	Tidak ada perubahan risiko atau isu eksternal & internal.	-	Lakukan pemantauan secara berkala.

4. Ketidaksesuaian Dan Tindakan Korektif

Hasil audit internal dan pemantauan serta pengukuran atas pelaksanaan SMKI mengidentifikasi beberapa ketidaksesuaian (non-conformity) terhadap kebijakan internal dan standar ISO 27001 selama periode Semester II 2023, yaitu:

No.	Temuan	Klausul ISO	Tindak Lanjut	PIC & Target	Status	Arahan Ketua SMKI
1.	Dokumen Kebijakan & Prosedur belum dilakukan review secara berkala.	5.1	Tim SMKI secara berkala meninjau kebijakan dan prosedur bank saat ini, serta memeriksa kepatuhan terhadap regulasi yang berlaku di Indonesia.	Tim SMKI 30 Nov 2023	Closed	Lakukan pemantauan secara berkala.
2.	Belum adanya pemeriksaan user akses Sharing Bandwidth.	8.9	Tim SMKI telah melakukan koordinasi dan membuat perencanaan pemeriksaan user akses Sharing Bandwidth.	Tim SMKI 30 Nov 2023	Closed	Lakukan pemantauan secara berkala.

5. Pencapaian Sasaran Keamanan Informasi

Pencapaian sasaran (KPI) SMKI selama periode Semester II 2023 adalah:

No	Sasaran (KPI)	Periode	PIC	Target KPI	Aktual KPI Q1-Q2
1.	Menyediakan program kesadaran keamanan informasi	Tahunan		· Awareness training.	100%
2.	Review User Akses.	Triwulanan		· Berita Acara Review User.	100%
3.	Laporan Kepatuhan SMKI.	Semester		· Laporan Kepatuhan.	100%
4.	Daftar Risiko SMKI	Tahunan		· Daftar Risiko.	100%
5.	Perbaikan hasil audit internal SMKI	Tahunan		· Tindak lanjut temuan.	100%

6. Hasil Penilaian Risiko

Tim SMKI telah melakukan review seluruh daftar risiko keamanan informasi (risk register) dan asset informasi PT BPR BATU ARTOREJO. Proses review dilakukan pada Semester II 2023. Hasil review menyimpulkan tidak terdapat perubahan daftar risiko keamanan yang signfikan. Penilaian tingkat risiko dan mitigasi risiko yang ada saat ini masih relevan dan secara umum berjalan efektif.

7. Peluang Perbaikan Berkelanjutan

Tim SMKI menerima beberapa usulan atau umpan balik (feedback) untuk meningkatkan pelaksanaan SMKI, yaitu:

No.	Kategori Perbaikan	Usulan Perbaikan	Inisiator	Keterangan	Arahan Direktur
1.	Temuan audit	Perbaikan hasil temuan Audit Internal Tahun 2023.	Tim SMKI	Proses perbaikan temuan audit internal tahun 2023 masih dilakukan selama bulan Januari – Oktober 2023.	Segera lakukan perbaikan sesuai dengan temuan audit.
2.	Manajemen Risiko	Seluruh daftar risiko SMKI harus berada di level acceptance (100%).	Tim SMKI		Lakukan sesuai dengan ketentuan.
3.	SDM	Penambahan jumlah personel dan peningkatan kompetensi.	Tim SMKI	Proses pemantauan dan pendokumentasian keamanan informasi bank secara bank wide dilakukan oleh 1 personel.	Lakukan sesuai dengan ketentuan.

7. Peluang Perbaikan Berkelanjutan

Tim SMKI menerima beberapa usulan atau umpan balik (feedback) untuk meningkatkan pelaksanaan SMKI, yaitu:

No.	Kategori Perbaikan	Usulan Perbaikan	Inisiator	Keterangan	Arahan Direktur
4.	KPI SMKI	• Memasukan aspek SMKI pada komponen KPI bisnis PT BPR XXXXX	Tim SMKI	Contoh KPI SMKI yang detil dan menggunakan parameter yang mudah diukur, misalnya jumlah insiden keamanan < 3 kali per bulan. Tingkat availability aplikasi 99%.	Lakukan sesuai dengan ketentuan.
5.	Sosialisasi.	Sosialiasi Petunjuk Teknis Berbasis ISO 27001:2022 kepada seluruh personel TI secara rutin.	Tim SMKI	Sharing session mengenai pedoman & SOP SMKI ke personel TI setiap minggu atau sesuai jadwal rutin.	Lakukan sesuai dengan ketentuan.

PERBARINDO

Perhimpunan Bank Perkreditan Rakyat Indonesia

	RISK REGISTER	No Dok	:	PND.04.00/PERB-SMKI/XI/2023
		Tanggal	:	1-Nov-23
	LAYANAN. SHARING BANDWIDTH PERBARINDO	Versi	:	1.0 (satu)
		Halaman		19

No	Kategori Risiko	Skenario Risiko	Skor Dampak	Tingkat Dampak	Skor Kemungkinan	Tingkat Kemungkinan	Nilai Risiko	Tingkat Risiko	Rencana Penanganan Risiko (Risk Treatment	Deskripsi Rencana Penanganan Risiko (Risk Treatment Plan)	ISO 27001 Controls (Annex)	Risiko Residual	Kriteria Penerimaan Risiko	Pemilik Risiko
1	Keamanan Informasi	User memiliki hak administrator di PC atau laptopnya. User tersebut memiliki kemampuan untuk menginstal perangkat lunak apa pun sehingga berpotensi melanggar kebijakan/pedoman TI.	5	Critical	4	Likely	20	Extreme	Mitigate	Mengontrol alokasi dan penggunaan hak akses istimewa.	A5.1 Policies for information security	Low	Low	Ketua Tim SMKI
		Penggunaan software yang tidak sah dan pelanggaran lisensi.								Menerapkan pemisahan peran kontrol akses.	A5.15 Access Control			
										Meninjau hak akses istimewa secara teratur.	A8.1 User end point devices			
										Memberikan kebijakan untuk manajemen akses pengguna dan lisensi perangkat lunak.	A8.18 Use of privileged utility proorams			
		Keamanan Informasi sensitif ke pihak yang tidak berwenang karena kurangnya mekanisme keamanan yang diterapkan di titik akhir pengguna.								Menerapkan kontrol akses dan mekanisme otentikasi yang kuat (mis. Kata sandi).	A8.19 Installation of software on operational systems			
										Memberikan kebijakan klasifikasi data dan prosedur penanganannya.				
										Menerapkan software antimalware di komputer & perangkat seluler.				
										Membatasi akses ke jaringan nirkabel internal dan akses jarak jauh.				
										Menyediakan program kesadaran keamanan informasi.				
										Melarang data rahasia di meja karyawan tanpa pengawasan.				
										Menerapkan konfigurasi pengerasan keamanan standar.				
2	Keamanan Informasi	Akses tidak sah yang dilakukan oleh orang yang tidak berwenang.	5	Critical	4	Likely	20	Extreme	Mitigate	Menerapkan kontrol akses dan mekanisme otentikasi yang kuat (mis. Kata sandi).	A5.1 Policies for information security	Low	Low	Ketua Tim SMKI
										Memberikan kebijakan untuk akses pengguna dan manajemen kata sandi.	A5.15 Access Control			
		User ID milik pengguna yang sudah resign/mutasi digunakan oleh karyawan lain untuk mendapatkan akses tidak sah ke aplikasi & infrastruktur TI.								Melakukan program kesadaran keamanan informasi.	A6.5 Responsibilities after termination or change of emplovment			
										Meninjau hak akses pengguna secara teratur.				
										Memberikan prosedur pemutusan hubungan kerja / mutasi karyawan.				
3	Keamanan Informasi	Pencurian peralatan TI (misalnya laptop, pc, harddisk, dll) sehingga menimbulkan kerugian biaya dan hilangnya data sensitif.	5	Critical	3	Possible	15	Extreme	Mitigate	Menerapkan kontrol akses dan mekanisme otentikasi yang kuat (mis. Kata sandi).	A5.1 Policies for information security A5.15 Access Control A7.1 Physical security perimeters A7.2 Physical entry A7.3 Securing offices, rooms and facilities A7.4 Physical security monitorino	Low	Low	Ketua Tim SMKI
										Menerapkan kontrol akses fisik.	A7.5 Protecting against physical and environmental threats			
										Memberikan kebijakan untuk backup.	A7.6 Working in secure areas			
										Melakukan program kesadaran keamanan informasi.	A7.7 Clear desk and clear screen			
										Menyediakan prosedur insiden keamanan.	A8.2 Privileged access rights			
4	Keamanan Informasi	Perubahan perangkat lunak yang tidak sah	5	Critical	4	Likely	20	Extreme	Mitigate	Mengontrol alokasi dan penggunaan hak akses istimewa.	A5.1 Policies for information security	Low	Low	Ketua Tim SMKI
										Menerapkan pemisahan peran kontrol akses.	A5.15 Access Control			
										Meninjau hak akses istimewa secara teratur.	A8.18 Use of privileged utility proorams			
										Memberikan kebijakan untuk manajemen perubahan.	A8.19 Installation of software on operational systems			
										Melakukan program kesadaran keamanan informasi.				
5	Keamanan Informasi	Gangguan operasional karena virus atau perangkat lunak yang tidak sah	5	Critical	4	Likely	20	Extreme	Mitigate	Mengontrol alokasi dan penggunaan hak akses istimewa.	A5.1 Policies for information security A5.7 Threat intelligence A5.15 Access Control A8.7 Protection against malware A8.12 Data leakage prevention	Low	Low	Ketua Tim SMKI
										Menerapkan software antimalware di komputer & perangkat seluler.	A8.16 Monitoring activities			
										Melakukan update dan scan komputer secara berkala.	A8.18 Use of privileged utility programs			
										Melakukan program kesadaran keamanan informasi.	A8.19 Installation of software on operational systems			
										Menerapkan konfigurasi dan aplikasi pengerasan keamanan standar.	A.23 Web filtering			
6	Keamanan Informasi	Tidak ada pembuangan data sensitif yang tepat. Ada kemungkinan data sensitif bocor.	5	Critical	3	Possible	15	Extreme	Mitigate	Melakukan program kesadaran keamanan informasi.	A5.1 Policies for information security A5.12 Classification of information	Low	Low	Ketua Tim SMKI
										Menerapkan mekanisme pembuangan yang aman seperti penghancur kertas dan penyeka disk.	A6.13 Information security awareness, education and training			
										Menyediakan kebijakan untuk pembuangan data yang aman	A7.14 Secure disposal or re-use of equipment			
										Memberikan kebijakan untuk klasifikasi data dan prosedur penanganan.	A8.10 Information deletion			
										Menerapkan label "Confidential" pada data sensitif & rahasia.	A8.12 Data leakage prevention			
7	Keamanan Informasi	Celah keamanan tidak teridentifikasi karena konfigurasi keamanan yang tidak memadai.	4	High	4	Likely	16	Extreme	Mitigate	Melakukan uji kerentanan dan penetrasi keamanan secara teratur	A5.1 Policies for information security A8.8 Management of technical vulnerabilities	Low	Low	Ketua Tim SMKI
										Menerapkan konfigurasi dan aplikasi pengerasan keamanan standar.	A8.9 Configuration management			
										11Menyediakan prosedur untuk pengujian keamanan.	A8.33 Test information			
8	Keamanan Informasi	Log sistem tidak menangkap data yang diperlukan untuk memastikan jejak audit yang sesuai / lengkap.	4	High	4	Likely	16	Extreme	Mitigate	Menerapkan mekanisme dan informasi logging standar.	A5.1 Policies for information security A8.9 Configuration management	Low	Low	Ketua Tim SMKI
										Melakukan review log secara teratur.	A8.15 Logging			
										Menerapkan konfigurasi dan aplikasi pengerasan keamanan standar.	A8.16 Monitoring activities			
9	Keamanan Informasi	Protokol jaringan yang tidak aman (text plain) digunakan dalam aplikasi kritis.	4	High	3	Possible	12	High	Mitigate	Menerapkan enkripsi yang kuat (cryptography).	A5.1 Policies for information security	Low	Low	Ketua Tim SMKI
										Melakukan uji kerentanan dan penetrasi keamanan secara teratur	A8.21 Security of network services			
										Menerapkan konfigurasi dan aplikasi pengerasan keamanan standar.	A8.22 Segregation of networks			
										Menyediakan prosedur untuk pengembangan yang aman & pengujian keamanan.	A8.24 Use of cryptography			
10	Operasional	Kapasitas PC tidak memadai untuk melayani semua pengguna	4	High	3	Possible	12	High	Mitigate	Menyediakan prosedur untuk memantau kapasitas.	A5.1 Policies for information security A5.21 Managing information security in the information and communication technology (ICT) supply chain A7.10 Storage media	Low	Low	Ketua Tim SMKI
										Melakukan pengecekan berkala atas kapasitas aplikasi & infrastruktur IT dengan pihak ketiga.	A8.6 Capacity management			
11	Operasional	Pemadaman listrik rutin dari PLN (pemasok listrik utama).	4	High	3	Possible	12	High	Mitigate	Memberikan kebijakan untuk akses fisik & kontrol lingkungan	A5.1 Policies for information security	Low	Low	Ketua Tim SMKI
										Menerapkan dan memantau kesiapan UPS untuk perangkat kritis.	A7.11 Supporting utilities			
										Menyediakan dokumen BCP & DRP yang diperbarui.	A7.13 Equipment maintenance			
										Menguji DRP secara rutin.	A8.13 Information backup			
										Berkoordinasi dengan pihak ketiga terkait daya cadangan (genset, UPS).				
										Menyediakan prosedur insiden keamanan.				
12	Operasional	Generator listrik gagal menyediakan daya yang diperlukan untuk mendukung data center jika terjadi pemadaman listrik.	4	High	3	Possible	12	High	Mitigate	Memberikan kebijakan untuk akses fisik & kontrol lingkungan	A5.1 Policies for information security	Low	Low	Ketua Tim SMKI
										Menerapkan dan memantau kesiapan UPS untuk perangkat kritis.	A7.11 Supporting utilities			
										Menyediakan dokumen BCP & DRP yang diperbarui.	A7.13 Equipment maintenance			
										Menguji DRP secara rutin.	A8.13 Information backup			
										Berkoordinasi dengan pihak ketiga terkait daya cadangan (genset, UPS).				
										Menyediakan prosedur insiden keamanan.				
13	Operasional	Kesalahan konfigurasi menyebabkan kesalahan aplikasi/sistem.	4	High	4	Likely	16	Extreme	Mitigate	Menerapkan konfigurasi dan aplikasi pengerasan keamanan standar.	A5.1 Policies for information security	Low	Low	Ketua Tim SMKI
										Melakukan review konfigurasi secara berkala.	A8.8 Management of technical vulnerabilities			
										Menyediakan prosedur insiden keamanan.	A8.9 Configuration management			
14	Keamanan Informasi	Personel pihak ketiga menggunakan informasi rahasia atau akses pribadi untuk penggunaan mereka sendiri atau untuk maksud jahat.	4	High	3	Possible	12	High	Mitigate	Menerapkan perjanjian kontrak & NDA dengan pihak ketiga	A5.1 Policies for information security A5.2 Information security roles and resoonsibilities A5.3 Segregation of duties A5.4 Management resoonsibilities A5.5 Contact with authorities A5.33 Protection of records A6.4 Disciplinary process	Low	Low	Ketua Tim SMKI
										Menerapkan pemisahan peran kontrol akses.	A6.6 Confidentiality or non-disclosure aoreements			
										Meninjau hak akses pengguna secara teratur.	A6.8 Information security event reporting			
										Menerapkan mekanisme otentikasi yang kuat (yaitu kata sandi) pada data sensitif.	A8.2 Privileged access rights			
											A8.3 Information access restriction			
15	Keamanan Informasi	Karyawan outsourcing memiliki level ***High*** untuk mengakses aplikasi.	4	High	2	Unlikely	8	High	Mitigate	Menerapkan perjanjian kontrak & NDA dengan pihak ketiga	A5.1 Policies for information security A5.15 Access control A5.18 Access rights A5.19 Information security in supplier relationshios	Low	Low	Ketua Tim SMKI
										Menerapkan pemisahan peran kontrol akses.	A6.6 Confidentiality or non-disclosure aoreements			
										Meninjau hak akses pengguna secara teratur.	A8.2 Privileged access rights			
										Menerapkan mekanisme otentikasi yang kuat (yaitu kata sandi) pada data sensitif.	A8.3 Information access restriction			
											A8.5 Secure authentication			
16	Keamanan Informasi	Akses tidak sah yang dilakukan oleh orang yang tidak berwenang.	4	High	3	Possible	12	High	Mitigate	Menerapkan pemisahan peran kontrol akses.	A5.1 Policies for information security A5.11 Return of assets A5.15 Access control A5.18 Access rights	Low	Low	Ketua Tim SMKI
		Berbagi kartu akses. Kartu akses karyawan yang dihentikan / dipindahkan yang digunakan oleh karyawan lain untuk mendapatkan akses tidak sah ke ruang TI.								Meninjau hak akses pengguna secara teratur.	A5.19 Information security in supplier relationships			
17	Operasional	Kebakaran gedung	4	High	1	Rare	4	High	Mitigate	Menerapkan detektor asap & pemadam api.	A7.5 Protecting against physical and environmental threats A7.6 Working in secure areas	Low	Low	Ketua Tim SMKI
										Memberikan kebijakan & prosedur untuk pengendalian fisik & lingkungan	A7.8 Equipment siting and protection			
										Menyediakan prosedur insiden keamanan.	A7.9 Security of assets off-premises			
										Melaksanakan program kesadaran keamanan informasi.	A7.13 Equipment maintenance			
18	Operasional	Kegagalan pada komponen server / perangkat keras	4	High	4	Likely	16	Extreme	Mitigate	Menyediakan prosedur insiden keamanan.	A7.5 Protecting against physical and environmental threats A7.6 Working in secure areas A7.8 Equipment siting and protection A7.9 Security of assets off-premises	Low	Low	Ketua Tim SMKI
										Melakukan monitoring secara berkala terhadap aplikasi & Infrastruktur IT dengan pihak ketiga.	A7.13 Equipment maintenance			
19	Operasional	Bencana alam yang mengakibatkan kerusakan fisik pada fasilitas atau aset (banjir, letusan gunung berapi, gempa bumi, sambaran petir, dll).	4	High	2	Unlikely	8	High	Mitigate	Menyediakan prosedur insiden keamanan.	A5.1 Policies for information security A5.30 ICT readiness for business continuity	Low	Low	Ketua Tim SMKI
										Melakukan penilaian risiko secara berkala.	A8.33 Test information			
20	Operasional	Kategorisasi yang tidak sesuai dari insiden yang dilaporkan pengguna atau permintaan pengguna menyebabkan ringkasan laporan insiden tidak valid.	3	Medium	4	Likely	12	High	Mitigate	Menyediakan prosedur insiden keamanan.	A5.1 Policies for information security A5.24 Information security incident management planning and preparation	Low	Low	Ketua Tim SMKI
										Melakukan program kesadaran keamanan informasi.	A6.3 Information security awareness, education and training			
21	Keamanan Informasi	Personel pihak ketiga bekerja di wilayah kerja karyawan.	3	Medium	2	Unlikely	6	Medium	Mitigate	Menerapkan pemisahan peran kontrol akses.	A7.1 Physical security perimeters A7.2 Physical entry A7.3 Securing offices, rooms and facilities	Low	Low	Ketua Tim SMKI
										Meninjau hak akses pengguna secara teratur.	A7.4 Physical security monitorino			
										Menerapkan perjanjian kontrak & NDA dengan pihak ketiga	A7.5 Protecting against physical and environmental threats			
										Menerapkan CCTV & area resepsionis berawak.	A7.6 Working in secure areas			
										Memberikan kebijakan & prosedur untuk manajemen akses pengguna termasuk akses pihak ketiga	A7.7 Clear desk and clear screen			
										Menyediakan prosedur insiden keamanan.	A8.2 Privileged access rights			
22	Keamanan Informasi	Banyak switch, hub atau titik akses nirkabel yang tidak terdeteksi. Memperkenalkan risiko akses tidak sah ke jaringan internal.	3	Medium	2	Unlikely	6	Medium	Mitigate	Memberikan kebijakan untuk jaringan nirkabel.	A7.11 Supporting utilities A7.12 Cabling security A7.13 Equipment maintenance	Low	Low	Ketua Tim SMKI
										Menerapkan pemisahan peran kontrol akses.	A8.20 Networks security			
										Melakukan program kesadaran keamanan informasi.	A8.22 Segregation of networks			
23	Keamanan Informasi	Terjadinya insiden dan masalah yang tidak dapat diselesaikan.	3	Medium	3	Possible	9	High	Mitigate	Menyediakan prosedur untuk memonitor aplikasi & Infrastruktur IT.	A5.1 Policies for information security A5.24 Information security incident management planning and preparation A5.25 Assessment and decision on information security events	Low	Low	Ketua Tim SMKI
										Menyediakan prosedur insiden keamanan.	A5.26 Response to information security incidents			
										Melakukan review berkala atas aplikasi & infrastruktur IT dengan pihak ketiga.	A5.27 Learning from information security incidents			
24	Project / Pengembangan	Ketidaktersediaan staf TI utama.	3	Medium	2	Unlikely	6	Medium	Mitigate	Memberikan kebijakan pengelolaan sumber daya manusia.	A5.2 Information security roles and resoonsibilities A5.3 Segregation of duties A5.4 Management resoonsibilities	Low	Low	Ketua Tim SMKI
										Memberikan program pelatihan untuk meningkatkan kompetensi & skill.	A6.3 Information security awareness, education and training			
										Melakukan review secara berkala terhadap recruitment dan man power plan.				
25	Project / Pengembangan	Pengguna tidak siap untuk menggunakan aplikasi/teknologi baru	3	Medium	3	Possible	9	High	Mitigate	Menyediakan prosedur untuk pengembangan yang aman.	A5.1 Policies for information security A8.26 Application security requirements A8.29 Security testing in development and acceptance	Low	Low	Ketua Tim SMKI
										Memberikan kebijakan untuk manajemen perubahan.				
										Melakukan review berkala (QA) atas pengembangan / dokumentasi proyek.				
										Menyediakan program pelatihan & pedoman manual bagi pengguna				
26	Operasional	Teknologi TI yang digunakan sudah usang dan tidak dapat memenuhi persyaratan bisnis baru (misalnya, jaringan, keamanan, penyimpanan)	2	Low	2	Unlikely	4	Low	Mitigate	Menyediakan prosedur untuk pengembangan yang aman.	A5.9 Inventory of information and other associated assets A8.10 Information deletion A8.26 Application security requirements	Low	Low	Ketua Tim SMKI
										Memberikan kebijakan untuk manajemen perubahan.				
										Melakukan review berkala (QA) atas pengembangan / dokumentasi proyek.				
27	Sumber daya manusia	Kurangnya keahlian TI terutama teknologi baru.	4	High	3	Possible	12	High	Mitigate	Memberikan kebijakan pengelolaan sumber daya manusia.	A5.1 Policies for information security A5.2 Information security roles and resoonsibilities A5.3 Segregation of duties A5.4 Management resoonsibilities A6.3 Information security awareness, education and training	Low	Low	Ketua Tim SMKI
										Memberikan program pelatihan untuk meningkatkan kompetensi & skill.				
										Melakukan review secara berkala terhadap recruitment dan man power plan.				
										Mengevaluasi pencapaian aktual & NCR				

PETUNJUK TEKNIS
PENGAMANAN INFORMASI
BERBASIS ISO 27001:2022
SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI)
PEMANFAATAN DATA KEPENDUDUKAN DITJEN DUKCAPIL MELALUI METODE AKSES ONLINE (WEB PORTAL & WEB SERVICE) DAN OFFLINE (CARD READER) DALAM MENDUKUNG LAYANAN PERBANKAN
PT BPR BATU ARTOREJO
ANGGOTA JARINGAN BERSAMA (SHARING BANDWIDTH) PERBARINDO

VERSI: 1.0 – AGUSTUS 2023

TIM SMKI PERBARINDO – BPR/BPRS

INFORMASI DOKUMEN & LEMBAR PERSETUJUAN

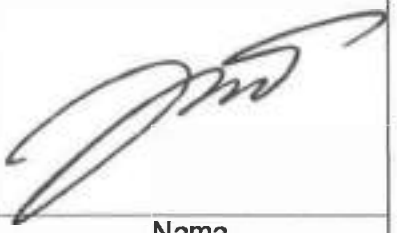
Nomor Dokumen : SOP.08.00/PND.01.00/601786/VIII/2023

Tanggal : 10 Agustus 2023

Versi : 1.0 (satu)

Klasifikasi :**TERBATAS**

TABEL KONTROL				
Versi	Dibuat oleh	Paraf	Di*review* oleh	Paraf
1.0	Puspita Ratnasarii		Wahyudin	

Dibuat oleh	Direview oleh	Disahkan oleh
Tgl: 01 Agustus 2023	Tgl: 08 Agustus 2023	Tgl: 10 Agustus 2023
		
Nama ANGGOTA TIM SMKI BPR	Nama KETUA TIM SMKI BPR	Nama DIREKTUR UTAMA BPR

DAFTAR ISI

BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam rangka mendukung bisnis dan menjaga keamanan informasi milik nasabah & bank, DPP PERBARINDO dan PT BPR BATU ARTOREJO. memandang perlu menyusun Petunjuk Teknis Pengamanan Informasi Berbasis ISO 27001 SMKI Layanan Jaringan Bersama (Sharing Bandwidth) yang selaras yang selaras dengan ketentuan yang berlaku tentang pemanfaatan data kependudukan Ditjen Dukcapil, Perbankan, ISO 27001:2022 Information Security Management System dan kebijakan internal PT BPR BATU ARTOREJO.

Petunjuk Teknis Pengamanan Informasi Berbasis ISO 27001 SMKI Layanan Jaringan Bersama (Sharing Bandwidth) ini memberikan panduan bagi PT BPR BATU ARTOREJO dan pihak terkait lainnya dalam melindungi aset informasi PT BPR BATU ARTOREJO terhadap risiko kerusakan, kehilangan dan berbagai ancaman keamanan lainnya baik dari internal maupun eksternal.

1.2. Landasan Hukum

1. Undang-undang No.40 tahun 2007 Tentang Perseroan Terbatas.
2. Undang-undang No.7 Tahun 1992 Tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998.
3. Undang-undang No.4 Tahun 2023 Tentang Pengembangan dan Penguatan Sektor Keuangan.
4. Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

5. Peraturan Otoritas Jasa Keuangan (POJK) Nomor 75 /POJK.03/2016 Tentang Standar Penyelenggaraan Teknologi Informasi Bagi Bank Perkreditan Rakyat Dan Bank Pembiayaan Rakyat Syariah.
6. Surat Edaran Otoritas Jasa Keuangan Nomor 15/SEOJK.03/2017 tentang Standar Penyelenggaraan Teknologi Informasi bagi Bank Perkreditan Rakyat dan Bank Pembiayaan Rakyat Syariah.
7. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi.
8. Peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 8 Tahun 2020 Tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik.
9. Surat Edaran Kementerian Dalam Negeri RI Direktorat Jenderal Kependudukan dan Pencatatan Sipil Nomor 470/15017/Dukcapil Tahun 2022 Tentang Penyelenggaraan Pemanfaatan Data Kependudukan.
10. Surat Edaran Kementerian Dalam Negeri RI Direktorat Jenderal Kependudukan dan Pencatatan Sipil Nomor 400.8/11759/Dukcapil Tahun 2023 Perihal Tanggapan atas Surat Perbarindo.
11. Akta notaris nomor 05 tertanggal 03 Maret 2021 yang dibuat dihadapan JOHNY WAISAPY Sarjana Hukum, Notaris di Batu.
12. Dokumen Standard Operating Procedure (SOP) Pemanfaatan Data Kependudukan DItjen Dukcapil melalui Jaringan Bersama (Sharing Bandwidth) Perbarindo.
13. SNI/ISO 27001:2022 mengenai Sistem Manajemen Keamanan Informasi.

1.3. Tujuan dan Sasaran

Tujuan dan sasaran Petunjuk Teknis ini adalah sebagai pedoman penerapan Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO 27001 pada Layanan Jaringan Bersama (Sharing Bandwidth) lingkungan PT BPR BATU ARTOREJO agar informasi dan aset kritikal milik anggota terlindungi dari risiko atau ancaman keamanan yang merugikan anggota & PERBARINDO.

1.4. Ruang Lingkup

Ruang lingkup Petunjuk Teknis Pengamanan Informasi Berbasis ISO 27001 SMKI ini terdiri dari:

1. Ketentuan Penggunaan Komputer.
2. Ketentuan Akses Pengguna.
3. Ketentuan *Antimalware*.
4. Ketentuan Penghancuran Data.
5. Ketentuan Klasifikasi, Penanganan dan Pelabelan Informasi.
6. Ketentuan Clear Desk and Clear Screen.
7. Ketentuan Manajemen Insiden.
8. Ketentuan Web Filtering.
9. Ketentuan Enkripsi.
10. Ketentuan Pengelolaan *Password*.
11. Ketentuan Keamanan Fisik dan Lingkungan.
12. Ketentuan Manajemen Risiko.
13. Ketentuan Pengelolaan Jasa Pihak Ketiga.
14. Ketentuan Keamanan Sumber Daya Manusia.
15. Ketentuan Tindakan Korektif dan Preventif.
16. Ketentuan Internal Audit SMKI.
17. Ketentuan Pelatihan dan Security Awareness.
18. Ketentuan Pelaporan.

Ketentuan ini berlaku untuk sistem operasi, aplikasi, database, server, perangkat keamanan dan jaringan, aset IT dan dokumen yang terkait dengan pemanfaatan data kependudukan Ditjen Dukcapil yang diakses melalui Jaringan Bersama (Sharing Bandwidth). Ketentuan ini juga berlaku untuk karyawan (tetap & kontrak) dan non-karyawan (pihak ketiga) yang memerlukan akses tersebut.

1.5. Pengertian dan Istilah

1. **Bank** adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup Masyarakat.

2. **BPR (Bank Perekonomian Rakyat) / BPRS (Bank Perekonomian Rakyat Syariah)** sebelumnya bernama Bank Perkreditan Rakyat/ Bank Pembiayaan Rakyat Syariah adalah lembaga keuangan bank yang melaksanakan kegiatan usaha secara konvensional atau berdasarkan prinsip syariah yang dalam kegiatannya tidak memberikan jasa dalam lalu lintas pembayaran.
3. **Direksi** adalah organ Bank yang berwenang dan bertanggung jawab penuh atas pengurusan Bank untuk kepentingan Bank, sesuai dengan maksud dan tujuan Bank serta mewakili Bank, baik di dalam maupun di luar pengadilan dan memiliki kewenangan lainnya sesuai dengan ketentuan anggaran dasar.
4. **PERBARINDO** adalah Perhimpunan Bank Perkreditan Rakyat Indonesia (dikenal juga sebagai Perhimpunan Bank Perekonomian Rakyat Indonesia) yang bersifat independen berdasarkan Pancasila dan Undang-Undang Dasar 1945 dan mempunyai anggota BPR-BPRS yang berada di seluruh wilayah kesatuan Republik Indonesia.
5. **DPP PERBARINDO** adalah Dewan Pengurus Pusat Perbarindo.
6. **Ditjen Dukcapil** adalah Direktorat Jenderal Kependudukan dan Pencatatan Sipil.
7. **Data Kependudukan** adalah data perseorangan atau data agregat yang terstruktur sebagai hasil dari kegiatan pendaftaran penduduk dan pencatatan sipil. Data kependudukan meliputi informasi mengenai identitas diri, status kependudukan, hubungan keluarga, dan peristiwa kependudukan.
8. **Jaringan Bersama (Sharing Bandwidth)** adalah salah satu layanan PERBARINDO untuk mengakses data kependudukan Ditjen Dukcapil.
9. **Accountability – akuntabilitas** adalah mekanisme untuk menilai tanggung jawab atas pengambilan keputusan dan tindakan.
10. **Audit Trail – Jejak Audit** adalah file pada komputer yang menyimpan informasi mengenai kegiatan pengguna (*User*) atau komputer, yang tersimpan secara kronologis, yang dapat digunakan untuk audit atau penelusuran.
11. **Authentication – Otentikasi** adalah proses atau aktivitas untuk membuktikan sesuatu itu benar, asli atau valid.
12. **Back Door** adalah metode untuk melewati otentikasi normal atau fitur pada sistem komputer yang memungkinkan akses data tanpa izin.

13. **Access – akses** adalah suatu usaha untuk membuka suatu saluran komunikasi dengan perangkat keras atau perangkat lunak tertentu, seperti modem yang digunakan untuk membuka akses internet. Perangkat keras atau perangkat lunak tersebut selain untuk memberikan data juga digunakan untuk menerima data untuk disimpan.
14. **Enkripsi** adalah alat untuk mencapai keamanan data dengan menerjemahkannya menggunakan *password*. Enkripsi mencegah *password* atau key supaya tidak mudah dibaca pada file konfigurasi.
15. ***Firewall*** adalah peralatan untuk menjaga keamanan jaringan yang melakukan pengawasan dan penyeleksian atas lalu lintas data atau informasi melalui jaringan serta memisahkan jaringan privat dan publik. Peralatan ini dapat digunakan untuk melindungi komputer yang telah dikoneksikan dengan jaringan dari serangan yang dapat merusak komputer internal dan menyebabkan data *corrupt*ion dan/atau *Denial of Service* bagi pengguna yang diotorisasikan.
16. ***Hardcopy*** adalah salinan data atau informasi komputer dalam bentuk tercetak atau dikenal dengan print out.
17. ***Password*** adalah kode atau simbol khusus untuk mengamankan sistem komputer yaitu untuk mengidentifikasi pihak yang mengakses data, program atau aplikasi komputer yang digunakan.
18. ***Patch*** adalah sekumpulan kode yang ditambahkan pada perangkat lunak untuk memperbaiki suatu kesalahan, biasanya merupakan koreksi yang bersifat sementara di antara dua keluaran versi perangkat lunak.
19. **Pengamanan Fisik** adalah suatu sistem pengamanan untuk mencegah akses oleh pihak-pihak yang tidak berwenang terhadap area komputerisasi serta peralatan atau fasilitas pendukung.
20. **Pengamanan Logic** adalah suatu sistem pengamanan untuk mencegah akses oleh pihak-pihak yang tidak berwenang terhadap sistem komputer dan informasi yang tersimpan di dalamnya yang antara lain meliputi penggunaan *User* ID dan *password*.
21. **Phising** adalah salah satu bentuk teknik social engineering untuk memperoleh informasi RAHASIA seseorang secara ilegal. Phising dapat dalam bentuk surat elektronik palsu yang seolah-olah berasal dari Bank atau perusahaan kartu kredit untuk memperoleh informasi seperti PIN dan *password*.

22. **Power *User*** adalah *User* ID yang memiliki kewenangan sangat luas.
23. **Sistem Manajemen Keamanan Informasi (SMKI)** adalah suatu sistem manajemen yang terdiri dari perencanaan, desain, implementasi, evaluasi dan pemeliharaan proses serta pengendalian risiko keamanan untuk menjaga Kerahasiaan, integritas serta ketersediaan aset-aset informasi.
24. **Metode Akses Dukcapil** adalah suatu metode akses data kependudukan yang disediakan oleh Ditjen Dukcapil baik secara online maupun offline.
25. **Metode Akses Dukcapil Online** adalah metode akses data kependudukan berbasis Web Portal dan Web Service.
26. **Metode Akses Dukcapil Offline** adalah metode akses data kependudukan dengan menggunakan alat baca KTP Elektronik (Card Reader).

BAB II
PENANGGUNG JAWAB DAN PIHAK/UNIT TERKAIT

2.1. Penanggung Jawab dan Pihak/Unit Terkait.

Tugas, wewenang dan tanggung jawab pihak/unit terkait akses Pemanfaatan Data Kependudukan Ditjen Dukcapil melalui Jaringan Bersama (Sharing Bandwidth).

1. **Direksi** memiliki tugas, wewenang dan tanggung jawab untuk:
   a. Mengesahkan kebijakan, pedorman, dan prosedur keamanan informasi Jaringan Bersama (Sharing Bandwidth).
   b. Memastikan kebijakan, standar, dan prosedur keamanan informasi Jaringan Bersama (Sharing Bandwidth) diterapkan secara efektif pada satuan kerja pengguna dan penyelenggara teknologi informasi dikaji ulang dan direvisi secara berkala.
   c. Menerapkan dan mengevaluasi Sistem Manajemen Keamanan Informasi (SMKI) yang efektif dan dikomunikasikan kepada satuan kerja pengguna.
   d. Menetapkan pembagian tugas dan tanggung jawab organisasi teknologi informasi dan keamanan informasi.
   e. Menetapkan tingkat risiko teknologi informasi Jaringan Bersama (Sharing Bandwidth) yang dapat diterima oleh Bank.
2. **Ketua SMKI dan Tim SMKI** memiliki tugas, wewenang dan tanggung jawab sesuai Surat Keputuhan (SK) Direksi dan Pengangkatan SMKI.
3. **Unit Kerja Kantor Pusat yang Melakukan Fungsi Operasional** memiliki tugas, wewenang dan tanggung jawab untuk**:**
   a. Menerapkan dan monitoring pelaksanaan SMKI di unit dibawahnya.

b. Menerapkan ketentuan keamanan pada proses operasional.
c. Mengelola aset sesuai ketentuan dan peraturan Bank.

4. **Unit Kerja Kantor Pusat yang Melakukan Fungsi SDM (Sumber Daya Manusia)** memiliki tugas, wewenang dan tanggung jawab untuk
   a. Menerapkan pemeriksaan latar belakang calon karyawan untuk meminimalkan risiko serangan dari sumber internal.
   b. Memfasilitasi dalam bentuk training kepada karyawan dari mulai perekrutan dan minimal satu kali per tahun mengenai kesadaran keamanan informasi.
   c. Memastikan bahwa karyawan mengakui secara tertulis bahwa mereka telah membaca dan memahami kebijakan keamanan informasi perusahaan.
   d. Menerapkan pengendalian keamanan pada proses karyawan mutasi dan berhenti untuk mencegah penyalahgunaan akses dan data.
   e. Menerapkan dan monitoring pelaksanaan SMKI di unit dibawahnya.

5. **Audit Internal** memiliki tugas, wewenang dan tanggung jawab sesuai Surat Keputuhan (SK) Direksi dan Pengangkatan SMKI.

2.2. Mitigasi Risiko atau Prinsip Kehati-hatian

Untuk mitigasi risiko dan prinsip kehati-hatian terkait dengan pemanfaatan data kependudukan Ditjen Dukcapil melalui Jaringan Bersama (Sharing Bandwidth) Tim SMKI perlu melakukan hal-hal berikut ini:

1. Tim SMKI melakukan evaluasi secara berkala, yaitu minimal setiap 1 (satu) tahun untuk menghindari risiko Petunjuk Teknis ini tidak sejalan dengan ketentuan serta perkembangan bisnis terkini.
2. Tim SMKI melakukan sosialisasi Petunjuk Teknis ini secara rutin minimal setiap 1 (satu) tahun atau jika ada perubahan kepada seluruh karyawan dan pihak terkait lainnya (apabila diperlukan).
3. Tim SMKI menerapkan prinsip kehati-hatian atas implementasi Petunjuk Teknis ini melalui pelaksanaan *review* atau audit oleh internal serta mengirimkan laporan kepatuhan setiap semester kepada PERBARINDO.

BAB III
KETENTUAN

3.1 Ketentuan Penggunaan Perangkat

Untuk semua penggunaan perangkat yang terkait dengan pemanfaatan data kependudukan Ditjen Dukcapil melalui Jaringan Bersama (Sharing Bandwidth).

3.1.1 Penggunaan PC, Laptop dan Perangkat Card Reader

1. Semua PC atau laptop Layanan Jaringan Bersama (Sharing Bandwidth) harus dikonfigurasi sesuai standar konfigurasi keamanan yang ditetapkan oleh Tim SMKI.
2. Penggunaan Card Reader harus sesuai dengan ketentuan yang tercantum pada perjanjian kerjasama dan Juknis yang ditetapkan oleh Ditjen Dukcapil.
3. Pengguna dilarang mengubah konfigurasi *hardware* dan *software* pada PC & laptop atau perangkat bergerak milik PT BPR BATU ARTOREJO. Jika membutuhkan perubahan konfigurasi, permohonan harus diajukan ke Tim SMKI sesuai Prosedur Manajemen Aset dan Petunjuk Teknis ini. Tim SMKI akan mengevaluasi dan menyimpan dokumentasi perubahan tersebut.
4. Pengguna dilarang menginstal *software* atau aplikasi apa pun yang tidak terdaftar dalam Standar Aplikasi PT BPR BATU ARTOREJO.
5. Pengguna dilarang menginstal *software* atau aplikasi yang tidak berlisensi atau diragukan keamanannya.
6. Pengguna dilarang melakukan *remote desktop* (*teleworking*) ke Layanan Jaringan Bersama (Sharing Bandwidth).
7. Jika Pengguna memerlukan *software* atau aplikasi tambahan, permohonan harus diajukan ke Tim SMKI.

8. Daftar Standar Aplikasi PT BPR BATU ARTOREJO yang telah disetujui harus di-*review* dan diperbarui secara rutin oleh Tim SMKI (lihat bagian 3.1.2).
9. Pengguna tidak diizinkan memiliki hak level administrator. Seluruh penggunaan hak level administrator harus disetujui oleh Tim Teknologi Informasi atau Tim SMKI.
10. *Software antimalware* harus di-install pada semua PC, laptop dan perangkat bergerak dengan database *signature* terbaru (lihat Ketentuan *Antimalware*).
11. Pengguna bertanggung jawab atas keamanan PC, laptop dan perangkat bergerak milik PT BPR BATU ARTOREJO dan harus menjaga atau membatasi akses fisik dan logik ke perangkat mereka.
12. Pengguna harus melakukan Keluar (logout) dari semua aplikasi atau mematikan PC & laptop saat ditinggalkan tanpa pengawasan untuk waktu yang lama.
13. Untuk mencegah akses tidak sah saat PCs, laptop dan perangkat bergerak ditinggalkan maka *screen saver* harus diaktifkan. Pengaturan *screen saver*, yaitu minimal 15 (limabelas) menit jika tidak melakukan aktivitas apa pun dan menggunakan perlindungan *password*.
14. Laptop dan perangkat bergerak tidak boleh ditinggalkan tanpa pengawasan di tempat umum dan harus dijaga saat bepergian.
15. Kehilangan laptop dan perangkat bergerak harus segera diinformasikan kepada Tim Teknologi Informasi atau Tim SMKI agar dilakukan tindakan pengamanan yang diperlukan.
16. Pengguna saat menyalin, memindahkan, atau menyimpan data RAHASIA & sensitif ke hard drive lokal dan media penyimpanan portable (seperti external hard drive, USB flash disk, dll) harus mengawasi dengan ketat. Semua karyawan dan non-karyawan (pihak ketiga) harus menandatangani perjanjian Kerahasiaan atau *Non-Disclosure Agreement* (NDA) terlebih dahulu saat mengakses atau bekerja di lingkungan PT BPR BATU ARTOREJO.

3.1.2 Ketentuan Standar Aplikasi PC atau Laptop

- Di bawah ini adalah standar aplikasi PC atau laptop yang berlaku untuk semua karyawan yang mengakses Layanan Jaringan Bersama (Sharing Bandwidth).
- Dalam keadaan tertentu, pengecualian terhadap ketentuan ini dapat diizinkan berdasarkan kebutuhan bisnis yang disetujui. Pengecualian terhadap Ketentuan

ini harus secara resmi didokumentasikan dan disetujui oleh Ketua Tim SMKI dan Direktur Utama atau Direktur Bidang Terkait (apabila diperlukan). Pengecualian tersebut akan di-*review* secara berkala.

No	Nama *Software*	Versi	Lisensi/Open Source/ Freeware	Pengguna
1	Windows	11 Pro 64 Bit	Lisensi	Semua Karyawan
2	Adobe Acrobat Reader DC	-	Open Source	Semua Karyawan
3	Google Chrome	-	Open Source	Semua Karyawan
4	Ms Office	2016	Lisensi	Semua Karyawan
5	McAfee		Lisensi	Semua Karyawan
6	Mozilla Firefox	Last *update*	Freeware	Semua Karyawan

3.1.3 Penggunaan Email

1. Tim Teknologi Informasi menyediakan fasilitas email dengan domain **@bprxxxx.com** atau domain yang sudah disetujui Direksi untuk mendukung komunikasi bisnis (misalnya gmail, yahoo, dan lainnya). Pengguna harus membatasi penggunaan email resmi untuk aktivitas pribadi.
2. Pengguna saat mengakses aplikasi email harus menggunakan koneksi yang aman dan terkini (HTTPS TLS) agar data email terlindungi.
3. PT BPR BATU ARTOREJO menghormati data privasi karyawan tetapi berhak untuk mengakses semua pesan email karena hal-hal berikut, namun tidak RAHASIA pada:
   a. Dalam rangka investigasi oleh lembaga penegak hukum atas tindakan pelanggaran atau yang melibatkan Pengguna.
   b. Untuk menyelesaikan insiden atau problem serta memfasilitasi pemulihan (*Recovery*) sistem email.
   c. Untuk pemeriksaan keamanan konten email dari ancaman virus.
4. Akses ke akun email milik karyawan hanya bisa dilakukan setelah mendapat persetujuan dari Direktur Utama atau Direktur Bidang Terkait.
5. Informasi sensitif & RAHASIA tidak boleh dikirimkan melalui email, kecuali dilindungi menggunakan enkripsi dan /atau *password*. Pengguna harus menandai email dengan label RAHASIA pada bagian Perihal/Subjek jika email

berisi informasi sensitif & RAHASIA (lihat Prosedur Klasifikasi, Penanganan & Pelabelan Informasi).

6. Jika karyawan mengirim email atau informasi lain milik PT BPR BATU ARTOREJO melalui Internet, nama karyawan atau alamat email PT BPR BATU ARTOREJO harus disertakan dalam setiap pesan sehingga karyawan bertanggung jawab atas semua pesan elektronik atau file yang berasal dari *User* ID atau alamat email mereka.
7. Pengguna dilarang mengirim atau meneruskan email dengan kategori dibawah ini:
   a. Email yang berisi komentar yang memfitnah, menyinggung, rasis, cabul atau tidak senonoh, hasutan, kejam, mengancam atau ofensif, menyebabkan perasaan permusuhan, kebencian, niat buruk antara orang-orang dari keyakinan atau keyakinan agama yang berbeda, jenis kelamin yang berbeda dan ras yang berbeda (SARA).
   b. Email yang berisi pesan yang dapat merusak reputasi PT BPR BATU ARTOREJO.
   c. Email yang berisi *malware*, seperti virus, *worm* dan trojan.
   d. Surat berantai seperti surat yang diteruskan dari rantai orang yang mengandung virus, tipuan, lelucon, kampanye pengumpulan dana amal, politik dan lainnya.
   e. Email yang tidak diminta dan dikirim ke sejumlah besar Pengguna dapat dianggap sebagai spamming email.
   f. Email berisi dokumen, perangkat lunak, atau informasi lain yang dilindungi oleh hak cipta, privasi, atau *Non-Disclosure Agreement* (NDA) yang dikirim tanpa persetujuan pemilik (owner).
   g. Surat kepada pihak eksternal yang berisi instruksi atau konten tanpa persetujuan PT BPR BATU ARTOREJO.
8. Dalam hal terjadi penyalahgunaan email, PT BPR BATU ARTOREJO dapat menghentikan akun email Pengguna dan mengambil tindakan hukum sesuai ketentuan yang berlaku.
9. Pengguna harus melindungi akun email mereka dan tidak berbagi dengan siapa pun.
10. Pengguna tidak boleh melampirkan file besar melebih ketentuan kuota email.

11. Pengguna tidak boleh menyamar menggunakan alamat email orang lain.
12. Pengguna tidak boleh memberikan informasi daftar email karyawan dari buku alamat email PT BPR BATU ARTOREJO kepada pihak yang tidak berwenang.
13. Pengguna tidak boleh mengirim atau membuat pernyataan yang salah atau menyesatkan, termasuk pernyataan atau kebijakan PT BPR BATU ARTOREJO yang salah atau tidak akurat.
14. Pengguna harus memahami risiko membuka file dokumen dengan makro atau menginstal program yang diterima melalui email.
15. Saat berkomunikasi dengan pihak luar, Pengguna harus menambahkan disclaimer pada pesan email untuk menjelaskan bagaimana informasi dalam email dapat digunakan dan memberitahu penerima tentang kewajiban mereka untuk tidak memproduksi ulang atau meneruskan email ke pihak lain. Standar disclaimer disediakan di bawah ini:

    PENYANGKALAN. Surat elektronik ini (termasuk lampirannya) hanya ditujukan untuk penerima dan dapat berisi informasi yang bersifat rahasia; Jika Anda bukan penerima yang dituju, Anda dengan ini diberitahukan bahwa penggunaan, pengungkapan, menyalin atau penyebaran surat elektronik ini dan lampiran apapun sangat dilarang dan Anda harus segera menghapusnya. Isi pesan dalam surat elektronik ini tidak selalu mencerminkan pandangan PT BPR BATU ARTOREJO. *Meskipun surat elektronik ini telah diperiksa agar bebas dari virus komputer,* PT BPR BATU ARTOREJO*tidak bertanggung jawab atas kerusakan yang disebabkan oleh virus apapun dan kode berbahaya yang ditularkan oleh surat elektronik. Oleh karena itu, penerima harus memeriksa lagi dari risiko virus, kode berbahaya, dll. sebagai akibat dari transmisi surat elektronik melalui internet.*

16. Untuk pengamanan sistem email, PT BPR BATU ARTOREJO menggunakan penyaringan *email, anti-spoofing, anti-SPAM, anti-relay dan anti malware* (virus).

3.1.4 Penggunaan Internet

1. Tim Teknologi Informasi menyediakan akses Internet kepada karyawan untuk meningkatkan kinerja dan membantu pekerjaan. Pengguna harus menggunakan Internet untuk tujuan bisnis PT BPR BATU ARTOREJO.
2. Pengguna terhubung ke Internet hanya melalui jalur atau media konektivitas

yang disediakan oleh PT BPR BATU ARTOREJO agar aman, terkontrol dan dimonitor.

3. Karyawan dan non-karyawan yang terhubung ke Internet tidak boleh secara terbuka mengungkapkan data RAHASIA atau informasi bisnis yang dapat mempengaruhi reputasi PT BPR BATU ARTOREJO.
4. Pengguna harus memastikan tidak ada informasi RAHASIA PT BPR BATU ARTOREJO yang diungkapkan di portal publik, milis, grup berita, dan situs web terkait lainnya.
5. Pengguna bertanggung jawab untuk melindungi akun dan *password* mereka.
6. Pengguna harus memahami resiko dan melakukan pemeriksaan terlebih dahulu jika mengakses situs web dengan mengklik tautan yang diterima melalui email atau situs web lain.
7. PT BPR BATU ARTOREJO berhak untuk memantau dan me*review* penggunaan internet untuk memastikan kepatuhan terhadap Ketentuan ini.
8. Pengguna dilarang mengirim data RAHASIA melalui media atau teknologi pesan pengguna akhir seperti *instant messaging, chat* tanpa dilindungi oleh enkripsi.
9. Pengguna jika menemukan penggunaan Internet yang tidak sah atau mencurigakan, seperti serangan oleh *Hacker*s harus segera melapor kepada Tim SMKI atau *Helpdesk*.
10. File yang diunduh dari Internet harus diperiksa (*scan*) secara menyeluruh oleh perangkat lunak *antivirus* yang disetujui PT BPR BATU ARTOREJO sebelum dibuka, digunakan, atau di-install.
11. Pengguna dilarang melakukan segala jenis kegiatan yang mengganggu jaringan PT BPR BATU ARTOREJO.
12. Aplikasi yang diakses melalui internet harus menggunakan minimal protokol HTTPS (HTTP over TLS) dan enkripsi yang kuat dan terkini, seperti public key 2048 bit, contohnya: https://perbarindo.or.id

3.1.5 Ketentuan Lisensi Perangkat Lunak

1. Tim SMKI menyediakan *software* berlisensi dalam jumlah yang memadai untuk membantu karyawan menyelesaikan pekerjaannya secara efektif.
2. Tim SMKI akan melakukan analisa jika *software* belum dimiliki oleh PT BPR BATU ARTOREJO maka akan dilanjutkan proses Pengadaan sesuai Prosedur Pengadaan Barang & Jasa.
3. Pemohon dan atasan langsung harus mengajukan permohonan kebutuhan *software* diluar standar ke Tim SMKI untuk membantu kegiatan operasonal.
4. Pengguna dilarang menggunakan *software* bajakan atau ilegal yang menyalahi perjanjian lisensi atau hak cipta.
5. *Software* milik pihak ketiga yang berada di PT BPR BATU ARTOREJO tidak boleh disalin kecuali mendapat persetujuan/tercantum pada perjanjian lisensi atau untuk kebutuhan *backup* sebagai bagian rencana BPC & DRP (kontinjensi).
6. *Software* yang diizinkan dipasang (install) pada komputer karyawan harus sesuai daftar Standar Aplikasi PT BPR BATU ARTOREJO.

3.1.6 Pelaporan Insiden

Setiap insiden keamanan yang diidentifikasi oleh Pengguna harus dilaporkan kepada Tim SMKI agar tindakan yang tepat dapat segera dilakukan. Laporan insiden harus dicatat dan disimpan oleh Tim SMKI.

3.1.7 Pemantauan Aktivitas dan Catatan (Log)

1. Pengguna harus menyadari bahwa sesuai dengan Prosedur Manajemen Insiden PT BPR BATU ARTOREJO, semua aktivitas pada sistem PT BPR BATU ARTOREJO akan terus dipantau dan dicatat. Catatan (log) tersebut disimpan dan diarsipkan. Jika diperlukan, catatan tersebut dapat digunakan sebagai bukti untuk tindakan hukum.
2. Catatan (log) harus diaktifkan pada sistem PT BPR BATU ARTOREJO dan jam pencatatan (log) harus dilakukan sinkronisasi (*clock synchronization*) dengan server acuan untuk menjamin akurasi catatan (log).
3. Email dan web browsing dimonitor oleh administrator untuk memantau penggunaan jaringan, mendeteksi ancaman virus, memfilter *email spam*, dan pengendalian keamanan informasi.
4. Pengguna dilarang melakukan kegiatan yang berpotensi membahayakan atau merusak aset informasi, seperti:
    a. Menghubungkan modem ke server tanpa persetujuan.
    b. Menyebarkan *malware* di sistem atau jaringan.
    c. Mencuri (*sniffing*) data di jaringan.
    d. Menebak (*brute-force*) *password*.
    e. Tindakan kriminal menggunakan komputer (*computer crime*).
    f. Menghapus atau memodifikasi data tanpa otoritas.
    g. Mengunduh atau mentransmisikan konten yang tidak sah.
    h. Menjalankan tool pemindaian (*scan*).
    i. Melewati (bypass) *access control*.
    j. Memanfaatkan atau mengeksploit *security vulnerability*.
    k. Menginstal atau menggunakan perangkat lunak yang tidak berlisensi.
    l. Vandalisme.
    m. Penipuan atau pencurian komputer.
    n. Akses tanpa izin ke data milik PT BPR BATU ARTOREJO.

3.2 Ketentuan Akses Pengguna Layanan Jaringan Bersama (Sharing Bandwidth)

3.2.1 Pendaftaran Akses Layanan Jaringan Bersama (Sharing Bandwidth)

1. Pemohon mengisi formulir permohonan *User* ID, menandatangani dan menyerahkan formulir kepada atasan langsung untuk di-*review*. Jika disetujui, Pemohon mengirimkan formulir ke Tim SMKI dan pemilik sistem (jika ada).
2. Dalam hal pembuatan *User* ID untuk konsultan atau pihak ketiga, pemohon adalah pemimpin proyek atau koordinator pihak ketiga. Pemohon harus me-*review* penggunaan *User* ID tersebut dan melaporkan kepada Tim SMKI segera jika proyek telah selesai atau kontrak telah berakhir.
3. Atasan langsung Pemohon bertanggung jawab untuk me-*review* apakah hak akses yang diminta tepat sesuai kebutuhan pekerjaan karyawan sebelum menyetujui formulir.
4. Direksi (*system owner*) me-*review* ulang permohonan dan memberikan hak akses yang sesuai. Selanjutnya, mengirimkannya ke Tim SMKI.
5. Tim SMKI menerima formulir. Selanjutnya memeriksa kelengkapan dan validitas data *P*emohon. Jika sesuai, meneruskan permohonan dilanjutkan.
6. Tim SMKI membuat akun dan menetapkan *password* secara acak (default).
7. Permintaan perubahan *User* ID dan hak akses diajukan oleh Pengguna ketika ia dipindahkan ke departemen lain atau lokasi kerja lain.
8. Tim SMKI berhak menonaktifkan *User* ID dan Pengguna harus mengajukan permohonan baru untuk *User* ID di departemen atau lokasi kerja baru.
9. Pengguna bertanggung jawab atas semua tindakan atau aktivitas yang dilakukan dengan *User* ID mereka pada sistem informasi PT BPR BATU ARTOREJO.

3.2.2 *Review* Pengendalian Akses Layanan Jaringan Bersama (Sharing Bandwidth)

1. Tim SMKI berkoordinasi dengan Pemilik Sistem (*system owner*) harus melakukan *review User* ID dan hak akses secara rutin, yaitu minimal setiap 1 (satu) bulan sekali. *Review* mencakup perubahan pemilik (jika ada), Pengguna aktif dan level akses serta aktivitas pengguna tersebut.
2. *User* ID yang tidak digunakan selama lebih dari 90 (sembilan puluh) hari harus dinonaktifkan oleh Tim SMKI setelah diverifikasi dengan Direksi (*system owner*).

3.2.3 Penonaktifan *User* ID Layanan Jaringan Bersama (Sharing Bandwidth)

1. *User* ID setiap karyawan yang telah berhenti dari PT BPR BATU ARTOREJO, seperti *resign*, pemutusan hubungan kerja dan pensiun, harus dihapus dari semua sistem PT BPR BATU ARTOREJO maksimal H+1 atau sehari setelah karyawan berhenti bekerja.
2. Setelah pemutusan hubungan kerja atau berakhirnya kontrak, semua karyawan (karyawan dan non-karyawan) harus mengembalikan semua aset TI yang mereka miliki, seperti namun tetapi tidak RAHASIA pada: komputer, kartu akses, token, kunci dan perangkat bergerak lainnya.
3. Tim SMKI setelah menerima laporan tersebut akan memeriksa (validasi) *User* ID dan hak aksesnya.
4. Tim SMKI akan menonaktifkan *User* ID dan hak akses yang tidak sesuai dan memperbarui daftar *User* ID.
5. Tim SMKI memberitahu Unit Kerja terkait mengenai penonaktifan *User* ID tersebut.
6. Tim SMKI wajib memberitahu atau melaporkan ke DPP PERBARINDO perubahan baik penambahan maupun pengurangan pengguna*/user* di BPR-BPRS dengan mengisi formulir yang sudah ditetapkan oleh DPP PERBARINDO setelah mendapat persetujuan dari Direksi, paling lambat 10 (sepuluh) hari setelah perubahan.

3.3 Ketentuan *Antimalware*

3.3.1 Instalasi dan Konfigurasi *Antivirus* (*antimalware*)

1. Semua komputer PC, laptop dan perangkat bergerak milik PT BPR BATU ARTOREJO yang terhubung ke harus terpasang (install) *software antivirus* yang digunakan untuk mengakses Layanan Jaringan Bersama (Sharing Bandwidth).
2. Semua karyawan dilarang mengubah pengaturan *antivirus*. Jika membutuhkan perubahan, karyawan harus menghubungi Tim SMKI.
3. Konfigurasi *software antivirus* harus diatur untuk melakukan pemindaian (*scan*) *real time* semua file saat diakses, disalin, atau dipindahkan.
4. Konfigurasi *software antivirus* harus diatur untuk mengkarantina file yang terinfeksi jika tidak dapat dibersihkan.

5. Tim SMKI harus me-*review software antivirus* untuk menilai kemampuan mendeteksi, menghapus dan melindungi dari *malware* yang berbahaya dan terkini.
6. Tim SMKI harus memonitor perangkat lunak *antivirus* berjalan aktif, memiliki *signature* terkini dan mampu menghasilkan log atau catatan.

3.3.2 Pembaruan *Antivirus Signature*

1. *Antivirus signature* terkini harus diimplementasikan segera secara otomatis (terjadwal) atau maksimal 1 (satu) bulan sejak dirilis jika dilakukan pembaruan secara manual.
2. Seluruh komputer PC, laptop dan perangkat bergerak milik PT BPR BATU ARTOREJO harus diperbarui dengan *antivirus signature* terkini yang terhubung ke Layanan Jaringan Bersama (Sharing Bandwidth).

3.3.3 Laporan Status *Antivirus*

1. *Software antivirus* harus melakukan pemindaian (*scan*) rutin minimal setiap minggu pada laptop dan PC untuk mendeteksi ancaman *malware*.
2. Laporan pemindaian (*scan*) *malware* harus tersedia. Tim SMKI harus melakukan pengecekan laporan *antivirus* minimal setiap bulan sebagai evaluasi efektivitas pengendalian *antimalware*.
3. Tim SMKI mendokumentasikan/menyimpan hasil review atas pengecekan antivirus setiap bulan.

3.3.4 Vulnerabilities dan *Malware* Baru

1. Tim SMKI harus secara teratur mengumpulkan informasi mengenai ancaman keamanan, *vulnerability* dan *malware* terbaru melalui berlangganan atau bergabung pada milis, forum spesialis keamanan, lembaga keamanan atau regulator.
2. Tim SMKI bertanggung jawab untuk menerapkan pengendalian keamanan untuk mencegah atau mendeteksi *vulnerability* dan *malware* terbaru pada sistem atau jaringan PT BPR BATU ARTOREJO.

3. Tim SMKI harus menginformasikan melalui email atau pesan singkat kepada seluruh karyawan tentang ancaman keamanan, *vulnerability* dan *malware* terbaru dan tindakan penanganannya.

3.3.5 Akses Pihak Ketiga

1. Pihak ketiga atau pihak eksternal PT BPR BATU ARTOREJO jika ingin menghubungkan komputer PC, laptop atau perangkat bergerak mereka ke jaringan PT BPR BATU ARTOREJO harus mendapatkan persetujuan Tim SMKI.
2. Sebelum terhubung ke jaringan PT BPR BATU ARTOREJO Tim SMKI melakukan pemeriksaan bahwa komputer atau perangkat bergerak tersebut terpasang (install) *software antivirus* dan *patch* keamanan terbaru serta hasil *scan* menunjukan bebas dari virus dan *malware* lainnya serta.

3.3.6 Pelaporan Insiden Virus

1. Semua karyawan dan non-karyawan harus melapor kepada Tim SMKI jika mengalami atau mengetahui indikasi adanya serangan *malware* pada komputer yang terhubung *ke* Layanan Jaringan Bersama (Sharing Bandwidth).
2. Tim SMKI harus melakukan Prosedur Insiden Keamanan untuk penanganan yang tepat.
3. Tim SMKI tidak bisa menangani serangan *malware* pada komputer yang terhubung *ke* Layanan Jaringan Bersama (Sharing Bandwidth), maka harus segera menghubungi Tim SMKI DPP PERBARINDO.

3.3.7 Perubahan *Software Antimalware*

Semua perubahan pada *software antivirus* harus mengikuti Panduan Teknis ini yang mencakup perubahan:

1. Upgrade *software antivirus*.
2. Perubahan arsitektur penempatan *software antivirus* atau jadwal pembaruan.
3. Penambahan/penghapusan komponen *antivirus*.

3.3.8 Kesadaran Pengguna

Tim SMKI harus melakukan sosialisasi mengenai ancaman *malware* dan prosedur keamanan informasi kepada seluruh karyawan secara rutin minimal 1 (satu) kali

setiap tahun. Tujuan sosialisasi agar Pengguna memahami bahaya yang disebabkan oleh *malware* dan ancaman keamanan lainnya serta ketentuan keamanan PT BPR BATU ARTOREJO yang harus dipatuhi.

3.4 Ketentuan Penghancuran Data

3.4.1 Persetujuan Penghancuran (Disposal)

1. Penghancuran aset informasi dan media harus mendapat persetujuan yang lengkap dari Direksi. Proses penghancuran aset informasi dan media (TI) harus dilakukan sesuai ketentuan Prosedur Pengendalian Informasi Terdokumentasi dan Prosedur Manajemen Aset.
2. Direksi wajib menandatangani dokumen penghancuran media atau aset informasi.
3. Proses penghancuran media dan aset informasi harus di lokasi yang aman dan mematuhi peraturan lingkungan.
4. Proses penghancuran media dan aset informasi harus dilaporkan dalam dokumen "Berita Acara Disposal Data" (format dokumen bisa dilihat pada lampiran). Laporan ini berisi jenis media yang dihancurkan, deskripsi data atau aset informasi, jumlah media dan data, klasifikasi data, tanggal penghancuran dan pelaksana penghancuran.

3.4.2 Penghancuran Dokumen Media Kertas

1. Apabila informasi dengan klasifikasi RAHASIA (label "RAHASIA") sudah tidak lagi berlaku karena persyaratan hukum atau jangka waktu penyimpanan telah melebihi ketentuan, maka informasi tersebut harus dihancurkan dengan aman.
2. Sebelum menghancurkan dokumen media kertas, Tim SMKI dan unit kerja terkait harus mengawasi dokumen tersebut.
3. Media kertas harus selalu dihancurkan dengan menggunakan alat penghancur kertas (*shredder*) atau dibakar (*incinerator*).
4. Semua limbah yang dihasilkan harus dihancurkan dan berada di lokasi yang aman.

3.4.3 Penghancuran Dokumen Media Elektronik

1. Sebelum menghancurkan media elektronik apapun, Tim SMKI dan unit kerja terkait bertanggung jawab untuk mengawasi data yang ada di dalamnya dan menghapusnya secara aman sehingga tidak ada data yang dapat dipulihkan, seperti data nasabah dan *software* berlisensi.
2. Media penyimpanan informasi seperti hard drive dan USB drive harus dihapus menggunakan *software* khusus pemformatan level rendah (misalnya standar DoD 5220.22-M).
3. Media penyimpanan yang kadaluwarsa atau rusak harus dihapus menggunakan *software* pemformatan tingkat rendah (misalnya Standar DoD 5220.22-M) sebelum dibuang.
4. Apabila data atau aset informasi tidak dapat dihapus menggunakan *software* pemformatan tingkat rendah (misalnya Standar DoD 5220.22-M), maka media itu harus dihancurkan secara fisik (misalnya pembakaran, pemotongan) agar tidak dapat dipulihkan dengan cara apa pun.

3.4.4 Penghancuran Aset TI`

1. Persetujuan dari Direksi terkait harus diperoleh sebelum melakukan penghancuran aset TI. Proses penghancuran aset TI harus dilakukan sesuai ketentuan prosedur SOP Manajemen Aset.
2. Tim SMKI memastikan *backup* file telah dilakukan (jika diperlukan).
3. Apabila aset TI tidak dapat dihapus menggunakan *software* pemformatan tingkat rendah (misalnya Standar DoD 5220.22-M), maka media itu harus dihancurkan secara fisik (misalnya pembakaran, pemotongan) agar data tidak dapat dipulihkan dengan cara apa pun.

3.4.5 Jangka Waktu Penyimpanan & Penghancuran

PT BPR BATU ARTOREJO harus mengikuti ketentuan penyimpanan data sesuai Prosedur Pengendalian Informasi Terdokumentasi dan Prosedur Manajemen Aset. Namun, jika media atau aset membutuhkan penghancuran segera maka harus dapat persetujuan Dewan Direksi.

3.5 Ketentuan Klasifikasi, Penanganan dan Pelabelan Informasi

3.5.1 Daftar Aset Informasi (Inventarisasi) Layanan Jaringan Bersama (Sharing Bandwidth)

1. Semua aset informasi Layanan Jaringan Bersama (Sharing Bandwidth) milik PT BPR BATU ARTOREJO harus diidentifikasi dan didaftarkan (inventarisasi) sesuai Prosedur Manajemen Aset.
2. Tim SMKI berkewajiban mengelola "Daftar Aset Informasi".
3. Daftar aset informasi (inventarisasi) harus diperbarui secara rutin, yaitu minimal 1 (satu) kali setiap tahun untuk memudahkan pengelolaan aset informasi.

3.5.2 Klasifikasi dan Pelabelan Informasi

1. PT BPR BATU ARTOREJO telah menentukan klasifikasi aset informasi menjadi 3 (tiga) kategori sesuai Prosedur Manajemen Aset, yaitu:
   a. **RAHASIA**. Informasi yang memiliki nilai sensitif dan signifikan bagi PT BPR BATU ARTOREJO, termasuk informasi pribadi yang berhubungan dengan personel dan hanya akan diungkapkan kepada orang yang secara khusus berwenang untuk menerima informasi tersebut.
   b. **TERBATAS**. Informasi yang tidak sensitif dan kurang memiliki nilai signifikan bagi PT BPR BATU ARTOREJO tetapi jika diungkapkan kepada pihak eksternal dapat menyebabkan kerugian.
   c. **BIASA (PUBLIK).** Informasi yang tidak sensitif dan tidak memiliki nilai yang signifikan serta jika diungkapkan di luar PT BPR BATU ARTOREJO tidak akan membahayakan bisnis PT BPR BATU ARTOREJO.
2. Informasi yang belum diklasifikasikan akan diperlakukan sebagai **TERBATAS** sampai Direktur Utama atau Direktur Bidang Terkait atau pemilik informasi dan Tim SMKI menentukan klasifikasi yang tepat.
3. Informasi milik pihak ketiga yang telah dipercayakan kepada PT BPR BATU ARTOREJO harus diperlakukan sebagai klasifikasi TERBATAS, kecuali jika kontrak atau perjanjian tertulis lainnya menentukan lain.
4. Informasi yang telah diklasifikasikan akan tetap dijaga hingga secara spesifik oleh Direktur Utama atau Direktur Bidang Terkait atau Pemilik Aset dan Tim SMKI menetapkan perubahan. Pengecualian untuk informasi yang telah ditetapkan

menjadi BIASA (PUBLIK) sesuai jangka waktu penyimpanan atau ketika suatu peristiwa tertentu terjadi.

3.5.3 Penanganan Informasi

1. Dokumen berisi informasi milik PT BPR BATU ARTOREJO harus memiliki label sesuai dengan klasifikasinya dan ditempatkan di bagian bawah dokumen.
2. Untuk pengiriman informasi RAHASIA melalui media elektronik, label klasifikasi harus ditandai pada judul perihal/subjek, misalnya Subjek: Hasil Kepuasan Pelanggan (RAHASIA).
3. Dokumen cetak dan salinannya yang tidak berlabel akan diperlakukan sebagai TERBATAS.
4. Ketika tidak digunakan atau tidak di bawah pengawasan langsung, dokumen RAHASIA atau media yang berisi informasi RAHASIA harus disimpan dalam lemari terkunci. Lemari harus terletak di area aman dan hanya dapat diakses oleh personel berwenang.
5. Informasi RAHASIA yang disimpan pada komputer hard disk drive atau media penyimpanan portabel harus dilindungi *password* atau dienkripsi.
6. Dalam situasi darurat, seperti saat evakuasi karena bencana alam, kebakaran, atau ancaman bom, informasi RAHASIA harus disimpan di lemari yang terkunci.
7. Dilarang memperbanyak informasi RAHASIA, seperti menyalin (copy) dan mencetak tambahan melalui printer komputer, kecuali diizinkan secara khusus oleh Pemilik Aset dan Tim SMKI.
8. Pemelihara informasi (kustodian) berwenang untuk melakukan *backup* informasi RAHASIA ke dalam media penyimpanan sebagai tugas kustodian untuk melindungi aset informasi.
9. Ketika informasi RAHASIA akan atau sedang dicetak (misalnya: menggunakan printer jaringan atau printer di lokasi yang jauh) maka printer tidak boleh dibiarkan tanpa pengawasan.
10. Pencetakan tanpa pengawasan hanya diizinkan apabila lokasi printer terlindungi secara fisik sehingga hanya orang yang berwenang yang bisa masuk.

3.5.4 Pengiriman atau Transmisi

1. Jika informasi RAHASIA dikirim maka harus dipastikan bahwa informasi tersebut hanya diserahkan kepada orang yang berwenang.
2. Permintaan harus diajukan oleh pengguna yang membutuhkan informasi RAHASIA via email atau surat tertulis. Permintaan tersebut harus disetujui oleh Direktur Utama atau Direktur Bidang Terkait, Pemilik Aset dan Tim SMKI.
3. Pengiriman fisik informasi RAHASIA harus menggunakan kurir terpercaya seperti kurir internal atau Layanan Pos yang aman.
4. Semua informasi RAHASIA yang dikirim melalui kurir harus disimpan dalam amplop tertutup, ditandai label RAHASIA dan diserahkan ke penerima yang berwenang. Bukti tanda terima harus dibuat untuk memastikan pengiriman tepat waktu dan penerima sesuai yang dituju.

3.5.5 Penyimpanan Data

1. Jangka waktu penyimpanan harus ditetapkan sesuai dengan jadwal penyimpanan data PT BPR BATU ARTOREJO dan peraturan yang berlaku.
2. Detail jangka waktu penyimpanan (retensi) aset informasi dan media tercantum pada lampiran Prosedur Pengendalian Informasi Terdokumentasi dan Prosedur Manajemen Aset.
3. Informasi yang sudah memenuhi jangka penyimpanan (retensi) harus dihancurkan dengan aman sesuai prosedur.

3.6 Ketentuan Clear Desk and Clear Screen

3.6.1 Label Dokumen dan Media

1. PT BPR BATU ARTOREJO menetapkan 3 (tiga) kategori klasifikasi aset informasi dan penamaan label untuk dokumen dan media (lihat Prosedur Klasifikasi, Penanganan dan Pelabelan Informasi):
   a. **RAHASIA**. Informasi yang memiliki nilai sensitif dan signifikan bagi PT BPR BATU ARTOREJO, termasuk informasi pribadi yang berhubungan dengan personel dan hanya akan diungkapkan kepada orang yang secara khusus berwenang untuk menerima informasi tersebut.

b. **TERBATAS**. Informasi yang tidak sensitif dan kurang memiliki nilai signifikan bagi PT BPR BATU ARTOREJO tetapi jika diungkapkan kepada pihak eksternal dapat menyebabkan kerugian.

c. **BIASA (PUBLIK).** Informasi yang tidak sensitif dan tidak memiliki nilai yang signifikan serta jika diungkapkan di luar PT BPR BATU ARTOREJO tidak akan membahayakan bisnis PT BPR BATU ARTOREJO.

2. Semua dokumen cetak (*hardcopy*) yang berisi informasi klasifikasi "RAHASIA" harus disimpan dalam lemari terkunci dengan akses RAHASIA dan lokasi aman.
3. Semua dokumen elektronik (softcopy) yang berisi informasi klasifikasi "RAHASIA" harus disimpan dengan aman pada sistem dengan *password* atau enkripsi.
4. Informasi yang belum memiliki klasifikasi harus diperlakukan sebagai TERBATAS sampai Direktur Utama atau Direktur Bidang Terkait atau Pemilik Aset Informasi dan Tim SMKI menentukan klasifikasi yang tepat.

3.6.2 Perlindungan Aset Informasi di Area Kerja

1. Selama jam kerja, informasi RAHASIA hanya berada pada lokasi dengan akses terbatas. Informasi RAHASIA di meja karyawan atau area kerja harus ditutup ketika orang yang tidak berwenang berada di area tersebut.
2. Setelah jam kerja, informasi RAHASIA harus disimpan pada lemari terkunci dengan akses RAHASIA dan di area aman.
3. Semua laporan, dokumen, media yang berisi informasi RAHASIA dan diedarkan di PT BPR BATU ARTOREJO harus diberi label RAHASIA.
4. Semua kertas atau kartu yang tidak digunakan harus dihancurkan menggunakan alat penghancur kertas (*shredder*).
5. Komputer dan printer tidak boleh dibiarkan logon saat tidak dijaga. Komputer dan printer harus dikunci menggunakan *password* atau screensaver dengan *password*. Komputer dan printer harus dikonfigurasi terkunci secara otomatis dalam waktu minimal 15 menit jika Pengguna tidak melakukan aktivitas apapun.
6. Setiap karyawan yang meninggalkan tempat kerja harus mengunci atau mematikan komputer mereka. Jika menggunakan OS Windows gunakan perintah CTRL + ALT + DEL untuk mengunci komputer.

7. Layar komputer harus ditutup atau dikunci (*screen saver*) dengan *password* ketika orang yang tidak berwenang berada dekat dengan layar saat mengerjakan informasi sensitif.
8. Semua media penyimpanan harus ditempatkan di lokasi yang aman pada lemari terkunci dan memiliki akses RAHASIA.
9. Papan tulis yang berisi informasi RAHASIA dan / atau sensitif harus dihapus.
10. *Password* tidak boleh disimpan pada catatan tempel yang dipasang di meja atau komputer.
11. Media penyimpanan seperti CDROM, DVD atau USB storage drive yang berisi data RAHASIA harus disimpan pada lemari terkunci.

3.7 Ketentuan Manajemen Insiden Keamanan Layanan Jaringan Bersama (Sharing Bandwidth)

Pengguna dan Tim SMKI harus mengikuti Prosedur Manajemen Insiden Keamanan ketika mengalami atau menangani insiden keamanan yang berhubungan dengan pemanfaatan data kependudukan melalui Jaringan Bersama (Sharing Bandwidth).

3.7.1 Peran Tim SMKI

1. Ketua Tim SMKI berperan sebagai otoritas pengatur untuk semua aktivitas insiden keamanan dan bertanggung jawab untuk komunikasi dengan Direktur Utama atau Direktur Bidang Terkait.
2. Ketua SMKI Informasi juga berperan sebagai Ketua tim insiden keamanan.
3. *Incident Handler*, yaitu personel Tim Teknologi Informasi atau Tim SMKI yang bertanggung jawab atas pengawasan investigasi insiden. *Incident Handler* akan menentukan apakah perlu menugaskan *Incident Response* Tim dan mengomunikasikan detail insiden kepada tim yang berpartisipasi.
4. Analis Insiden, yaitu personel Tim Teknologi Informasi atau Tim SMKI yang bertanggung jawab merespons insiden langsung dan melaporkannya kepada *Incident Handler*.
5. Pihak internal lainnya jika diperlukan untuk terlibat dalam penanganan insiden, seperti Fungsi Internal Audit, Fungsi Manajemen Risiko, dll.
6. Pihak eksternal jika dibutuhkan untuk membantu dalam menanggapi insiden yang signifikan. Pihak ini akan dihubungi berdasarkan insiden yang terjadi.

Contoh entitas eksternal adalah, namun tidak terbatas pada: Penyedia Layanan Internet (ISP), Vendor Solusi Keamanan, konsultan dan hukum penegakan hukum (misalnya BSSN dan Cyber Crime Polri).

3.7.2 Identifikasi Insiden

1. Insiden keamanan adalah tindakan melanggar ketentuan keamanan informasi PT BPR BATU ARTOREJO sehingga mengakibatkan turunnya kualitas layanan atau rusaknya aset kritikal PT BPR BATU ARTOREJO.
2. Tim SMKI bertanggung jawab untuk memonitor semua kegiatan dan insiden pada sistem PT BPR BATU ARTOREJO selama 24/7 dengan dukungan dari seluruh karyawan.
3. Berikut ini adalah kegiatan yang dikategorikan sebagai insiden:
   a. Upaya menyamar atau menipu sebagai Pengguna yang sah untuk mendapatkan akses ke sistem atau data.
   b. Penggunaan *wireless* yang tidak sah (ilegal).
   c. Pemberitahuan oleh *Firewall*/IPS /IDS mengenai adanya aktivitas mencurigakan atau berbahaya.
   d. Gangguan layanan yang tidak diinginkan, seperti *Denial of Service* (DOS).
   e. Kerusakan peralatan IT.
   f. Perangkat keras dan komponennya hilang atau dicuri.
   g. Serangan virus yang mengakibatkan kerugian atau terhentinya bisnis.
   h. Bencana alam.
   i. Penggunaan sistem yang tidak sah (ilegal) untuk pemrosesan atau penyimpanan data.
   j. Perubahan pada perangkat keras, sistem, firmware, *software* dan data tanpa sepengetahuan atau persetujuan pemilik (owner).
   k. Kegagalan sistem informasi dan layanan.
   l. Kehilangan informasi sensitif dan RAHASIA.
4. Waktu dan lokasi insiden harus diinformasikan kepada Tim SMKI agar insiden ditangani.
5. Tim SMKI dan semua Pengguna harus mengikuti panduan berikut dalam mengidentifikasi insiden keamanan:

a. Penggunaan sumber daya sistem yang tidak normal. Jika penggunaan CPU atau memori pada sistem sangat tinggi dibandingkan dengan penggunaan normal, sistem tersebut berpotensi telah di *compromised*. Sistem yang di *compromised* dapat dieksploitasi oleh penyerang (*attacker*) untuk menyebarkan virus atau menginfeksi sistem lain yang ditandai Penggunaan sumber daya yang tinggi. Insiden ini harus dilaporkan kepada Tim Teknologi Informasi atau Tim SMKI. Administrator sistem harus melacak penggunaan sumber daya dan menganalisa penyebab penggunaan tidak normal.

b. Respons lambat aplikasi. Pengguna bisa merasakan waktu response aplikasi menjadi sangat lambat jika server aplikasi atau jaringan telah di *compromised* dan digunakan untuk tujuan jahat. Serangan virus atau *worm* dapat menyebabkan gangguan jaringan sehingga response aplikasi menjadi lambat dan tidak stabil. Insiden ini harus dilaporkan kepada Tim SMKI.

c. Data hilang atau rusak (*corrupt*). Jika Pengguna mengidentifikasi bahwa data atau file yang disimpan pada komputer telah dihapus atau berubah tanpa sepengetahuan mereka. Hal ini bisa menjadi indikasi sistem telah di *compromised*. Insiden ini harus dilaporkan kepada Tim SMKI.

d. Perubahan konfigurasi computer. Jika konfigurasi komputer Pengguna terlihat berbeda, seperti terdapat aplikasi ilegal yang di-install, perubahan screensaver/ikon di layer, atau sistem menjalankan aplikasi tanpa perintah Pengguna maka hal ini bisa menjadi indikasi bahwa komputer mereka telah di *compromised*. Insiden ini harus dilaporkan kepada Tim SMKI.

e. Perubahan *password* dan *User* ID. Pengguna harus melapor kepada Tim SMKI jika menemukan *User* ID dan *password* mereka telah diubah tanpa sepengetahuan mereka. Hal ini dapat menjadi indikasi sistem telah *compromised*. Pengguna harus melapor jika mencurigai orang lain menggunakan akun mereka, seperti email, aplikasi atau data di posting dari akun mereka tanpa ijin. Insiden ini harus dilaporkan kepada Tim SMKI.

f. Infeksi virus. Pengguna harus melaporkan jika virus atau *worm* menginfeksi satu atau lebih komputer dan tidak bisa dibersihkan oleh *software antivirus* yang ada.

g. Perubahan aplikasi. Jika aplikasi yang diakses oleh Pengguna terlihat berbeda dari tampilan normalnya atau hak akses Pengguna dalam aplikasi telah dimodifikasi maka ada indikasi aplikasi mungkin telah di *compromised*.

h. Kelemahan keamanan terdeteksi. Jika Pengguna mendeteksi terdapat kelemahan keamanan aplikasi sehingga terjadi perubahan akses yang tidak sah maka insiden ini harus dilaporkan kepada Tim SMKI.

i. Pelanggaran oleh pihak lain. Jika Pengguna menemukan terdapat pelanggaran keamanan yang dilakukan oleh pihak lain seperti menjalankan program berbahaya, percobaan masuk ke sistem, melakukan tindakan kriminal, pelanggaran hak cipta atau lisensi, maka Pengguna harus melaporkan kejadian tersebut kepada Tim SMKI.

j. Akses ke data atau sistem tanpa otorisasi yang mencakup:
   - Penggunaan *User* ID dan hak akses secara tidak sah.
   - Akses tidak sah ke direktori, file, atau media.
   - Penempatan perangkat keras atau *software* '*sniffing*' pada segmen jaringan untuk mengambil data di jaringan.

k. Modifikasi data tanpa otorisasi yang meliputi:
   - Pengiriman file yang tidak sah.
   - Penyebaran trojan horse atau virus.
   - Penghapusan data.
   - Modifikasi data.
   - Perusakan halaman web.

l. Gangguan layanan atau gangguan aktivitas sistem yang meliputi:
   - Serangan *Denial of Service* terdistribusi (DDoS) melalui paket *flooding* sehingga menyebabkan hilangnya koneksi jaringan eksternal.
   - Eksploitasi *vulnerability* yang menyebabkan gangguan jaringan.
   - Kerusakan (*crash*) sistem.
   - Hilangnya konektivitas pada sistem.
   - Sistem gagal (*failure*) sebagian atau seluruhnya.
   - Kehilangan atau kerusakan sistem.

m. Perubahan pada *software*, *firmware* sistem atau perangkat keras tanpa persetujuan yang meliputi:

- Pemasangan kode *backdoor* tanpa ijin (pelanggaran oleh tim developer).
- Modifikasi kode sistem tanpa otorisasi.
- Modifikasi pemasangan kabel jaringan.
- Pemasangan *software* atau perangkat keras dengan tujuan jahat (misalnya *keystroke logging* atau *backdoor*).
- Pemindahan, penambahan, atau penggantian perangkat TI tanpa ijin.

n. Kegiatan Pemindaian (*scan*) tanpa persetujuan. Upaya untuk mendapatkan informasi yang dapat digunakan untuk melakukan serangan, seperti:
- Pemindaian (*scan*) sistem PT BPR BATU ARTOREJO.
- Pemindaian yang ditargetkan pada seluruh atau sebagian *IP address*.
- Serangan rekayasa sosial.
- Pertanyaan tentang kapabilitas / kerentanan jaringan oleh pihak yang tidak berwenang.
- Reset *password* yang tidak sah (ilegal).

o. Kehilangan atau kerusakan pada sistem PT BPR BATU ARTOREJO.

p. Aktivasi secara tidak sah oleh Pengguna ID yang dinonaktifkan.

q. Terdapat Pengguna ID yang tidak dikenal dan memiliki hak akses tinggi sebagai indikasi bahwa sistem telah diserang.

6. Pemeriksaan untuk mengidentifikasi keberadaan *wireless* harus dilakukan secara teratur. Jika terdeteksi adanya perangkat *wireless* yang tidak sah (ilegal), penyelidikan dan tindakan mematikan *wireless* harus segera dilakukan.

3.7.3 Cara Pelaporan Insiden

1. Jika Pengguna mencurigai adanya insiden keamanan pada sistem maka harus segera melapor kepada Tim SMKI
2. Pengguna tidak boleh melakukan pemeriksaan atau pengujian sendiri untuk membuktikan kelemahan atau insiden keamanan yang dicurigai terjadi karena dapat merusak layanan atau barang bukti.
3. Tim SMKI harus melakukan analisa awal untuk mengidentifikasi penyebab dan dampak kerusakan serta mengambil langkah-langkah yang diperlukan untuk menangani insiden tersebut.
4. Laporan insiden harus dibuat oleh Tim SMKI (*Incident Response Team*).

5. Jika Tim SMKI tidak bisa menangani insiden Layanan Jaringan Bersama (Sharing Bandwidth), maka harus segera menghubungi Tim SMKI DPP PERBARINDO.

3.7.4 Penilaian Insiden dan Verifikasi

1. Tim SMKI harus memeriksa validitas insiden. Pemeriksaan berdasarkan laporan kejadian dan bukti yang dikumpulkan sehingga tim memahami insiden dan dampaknya pada bisnis PT BPR BATU ARTOREJO.
2. Insiden harus diklasifikasikan berdasarkan matriks manajemen insiden dibawah ini:
   a. Insiden Prioritas 1 (*critical* atau *emergency*): gangguan harus dapat diselesaikan dalam waktu 4 jam. Insiden ini jika tidak ditangani bisa menjadi bencana major dengan area luas untuk periode waktu yang lama.
   b. Insiden Prioritas 2: gangguan harus dapat diselesaikan dalam waktu 1 hari kerja.
   c. Insiden Prioritas 3: gangguan harus dapat diselesaikan dalam waktu 2 sampai 5 hari kerja.
   d. Insiden Prioritas .4: gangguan dapat diselesaikan dengan menyesuaikan urutan/antrian.
3. Tim SMKI harus mencatat insiden dan mengalokasikan nomor insiden untuk memudahkan monitoring penangan insiden.
4. Setelah insiden diverifikasi, Tim SMKI (*Incident Response Team*) harus menyusun rencana penanganan insiden.
5. Rencana Penanganan Insiden harus diperbarui dan dipelihara oleh Tim SMKI sesuai dengan pengalaman dan perkembangan industri.
6. Berdasarkan informasi yang tersedia dan tingkat prioritas insiden,Tim SMKI (*Incident Response Team*) akan mengirimkan peringatan kepada Pengguna yang terkena dampak.
7. Jika Tim SMKI tidak bisa menangani insiden Layanan Jaringan Bersama (Sharing Bandwidth), maka harus segera menghubungi Tim SMKI DPP PERBARINDO.

3.7.5 Isolasi (*QuarantinelContainment*)

1. Strategi *containment* penting dilakukan untuk mencegah insiden menyebar luas atau meningkatkan kerusakan. Sebagian besar insiden memerlukan *containment*, sehingga Tim SMKI (*Incident Response Team)* perlu mempertimbangkan strategi *containment* dalam penanganan setiap insiden.
2. *Containment* juga berfungsi untuk menyediakan waktu bagi Tim SMKI (*Incident Response Team)* untuk mengembangkan strategi remediasi yang diperlukan.
3. Beberapa strategi *containment*, misalnya memutuskan computer/sistem dari jaringan, menonaktifkan tertentu fungsi. Keputusan *containment* perlu mempertimbangkan risiko yang acceptable dalam menangani insiden.

3.7.6 Pemulihan Insiden

1. Sesuai kategori dan dampak insiden, Tim SMKI (*Incident Response Team*) harus melakukan penanganan untuk memulihkan insiden.
2. Penanganan pemulihan bisa berupa mengurangi / menghilangkan penyebab insiden, seperti:
   a. Menerapkan pengendalian keamanan tambahan.
   b. Pemasangan *patch* baru.
   c. Restore data *backup*.
   d. Konfigurasi ulang perangkat keamanan, seperti *Firewall* dan IDS / IPS.
3. Setelah pemulihan dilakukan, perangkat monitoring keamanan tambahan harus dikonfigurasi untuk memastikan bahwa insiden bisa dicegah. Evaluasi pengendalian keamanan harus dilakukan mencakup pemasangan IDS / IPS tambahan, monitoring sistem dan pemeriksaan log aplikasi sistem yang terkena dampak.
4. Jika Tim SMKI tidak bisa menangani insiden Layanan Jaringan Bersama (Sharing Bandwidth), maka harus segera menghubungi Tim SMKI DPP PERBARINDO.

3.7.7 Pencegahan Insiden

1. Berdasarkan hasil penanganan insiden sebelumnya,Tim SMKI harus membuat rekomendasi tindakan pencegahan atau korektif untuk meningkatkan keamanan.

2. Tim SMKI harus menyimpan daftar rincian insiden yang berisi detail insiden dan solusi yang bisa menjadi rujukan sehingga solusi lebih cepat jika insiden yang sama atau serupa terjadi lagi.

3.7.8 Laporan Insiden

1. Laporan insiden keamanan yang pernah dan sedang terjadi (investigasi) harus dibuat serta disimpan oleh Tim SMKI.
2. Laporan insiden keamanan harus dijaga dan hanya bisa diakses oleh pihak yang berwenang.

3.7.9 Laporan Analisa Pasca Insiden

1. Tim SMKI harus menyusun laporan pasca insiden, pembelajaran yang diperoleh dari insiden dan efektivitas tindakan perbaikan yang diambil (korektif). Tim Tim SMKI harus melaporkan rincian insiden kepada Ketua Tim SMKI dan Direktur Utama atau Direktur Bidang Terkait (jika diperlukan).
2. Tim SMKI harus menilai efektivitas proses penanganan insiden dan mengidentifikasi perbaikan untuk mencegah insiden serupa.

3.8 Web Filtering

1. Seluruh akses internet yang dilakukan oleh pengguna dan pemroses Layanan Jaringan Bersama (Sharing Bandwidth) di PT BPR BATU ARTOREJO harus memiliki web filtering yang telah disetujui oleh PT BPR BATU ARTOREJO.
2. PT BPR BATU ARTOREJO harus memblokir akses pengguna ke situs web yang dianggap tidak aman atau tidak pantas.
3. PT BPR BATU ARTOREJO harus memastikan bahwa situs web yang diperbolehkan diakses oleh pengguna dan pemroses di PT BPR BATU ARTOREJO tidak mengandung konten yang melanggar hukum atau kebijakan PT BPR BATU ARTOREJO.
4. PT BPR BATU ARTOREJO harus memberikan akses internet yang cukup untuk memenuhi kebutuhan bisnis dan penggunaan pribadi yang wajar.
5. PT BPR BATU ARTOREJO harus mengimplementasikan perangkat lunak web filtering yang tepat untuk memblokir akses ke situs web yang dianggap tidak aman atau tidak pantas.

6. PT BPR BATU ARTOREJO harus memastikan bahwa perangkat lunak web filtering selalu diperbarui dengan definisi terbaru dari situs web yang dianggap tidak aman atau tidak pantas.
7. PT BPR BATU ARTOREJO harus melakukan pemantauan terhadap penggunaan internet oleh pengguna dan pemroses di PT BPR BATU ARTOREJO untuk memastikan kepatuhan terhadap kebijakan dan prosedur yang telah ditetapkan.
8. PT BPR BATU ARTOREJO harus memberikan pelatihan kepada seluruh pengguna dan pemroses di PT BPR BATU ARTOREJO tentang kebijakan dan prosedur web filtering.
9. Pelanggaran terhadap kebijakan dan prosedur web filtering akan ditangani oleh Tim SMKI sesuai dengan kebijakan disiplin dan hukuman yang berlaku di PT BPR BATU ARTOREJO.

3.9 Ketentuan Enkripsi

3.9.1 Enkripsi Informasi

1. Semua data RAHASIA dan sensitif Layanan Jaringan Bersama (Sharing Bandwidth) harus dienkripsi saat disimpan pada sistem atau dikirim melalui media apapun, seperti email, penyimpanan media portabel dan jaringan.
2. Semua akses ke sistem dan web aplikasi Layanan Jaringan Bersama (Sharing Bandwidth) harus menggunakan teknologi enkripsi, seperti SSH, VPN, atau TLS 1.2.
3. *Password* harus diacak selama transmisi dan saat disimpan pada sistem menggunakan kriptografi yang kuat.
4. Data nasabah yang sensitif harus menggunakan enkripsi dan protokol keamanan yang kuat seperti TLS 1.2 atau IPSEC untuk melindungi data di jaringan.

3.9.2 Pengelolaan Kunci Enkripsi

1. Setiap teknologi enkripsi yang digunakan Layanan Jaringan Bersama (Sharing Bandwidth) dietapkan oleh tim SMKI PERBARINDO.
2. Pada saat pemasangan (instalasi), enkripsi harus terpasang dan berjalan efektif.
3. Akses ke kunci enkripsi harus dibatasi hanya untuk personel tim SMKI PERBARINDO yang berwenang.

3.10 Ketentuan Pengelolaan *Password*

3.10.1 *Password*, PC, aplikasi, dan perangkat jaringan

1. *Password* harus memenuhi ketentuan sebagai berikut:
   a. Panjang *password* minimal 6 (enam) karakter dan maksimal 16 (enambelas).
   b. Berisi kombinasi karakter, angka, special karakter atau alphanumerik, huruf besar dan kecil.
2. *Password* tidak boleh ditampilkan atau dicetak.
3. Pengguna wajib mengubah *password* secara rutin, yaitu setiap 90 hari atau 3 bulan.
4. *Password* harus segera diubah jika ada kecurigaan bahwa *password* tersebut telah diketahui oleh pihak yang tidak berwenang.
5. Sistem harus mengatur riwayat *password* terakhir. Pengguna tidak diizinkan menggunakan *password* yang sama.
6. Sistem dan aplikasi harus melakukan pengecekan *password* lama sebelum mengijinkan Pengguna membuat *password* baru.
7. Sistem akan menonaktifkan *User* ID bila terjadi kesalahan sebanyak 3 (tiga) kali berturut-turut dalam memasukan *password* ke sistem informasi.
8. Sistem akan menonaktifkan *User* ID apabila *User* ID tidak digunakan selama jangka waktu 90 (Sembilan puluh) hari kalender berturut-turut.
9. Proses pengaktifan kembali *User* ID dilakukan oleh Tim SMKI setelah ada permohonan dari Pengguna mengenai pengaktifkan *User* ID.
10. Sistem dan aplikasi harus mencatat semua percobaan login yang gagal.
11. Kesalahan *password* harus dibatasi dan setelah itu *User* ID akan dikunci. Ketentuan penguncian *User* ID adalah:
    a. Jumlah percobaan gagal login maksimal pada server atau aplikasi adalah 3 (tiga) kali dan Pengguna akan terkunci selamanya hingga administrator membuka kunci sesuai ketentuan yang berlaku menggunakan formulir reset *User* ID.
    b. Koneksi ke server atau aplikasi akan terputus apabila Pengguna tidak melakukan aktivitas apapun lebih dari 15 menit.
12. Pengguna dilarang membagikan *password* miliknya kepada siapa pun.
13. Pengguna dilarang mencatat *password* dimanapun.

14. Riwayat perubahan *password* harus disimpan pada sistem.
15. *Password* yang disimpan pada dokumen cetak atau elektronik harus diklasifikasikan sebagai informasi RAHASIA. *Password* harus di enkripsi menggunakan kriptografi yang kuat pada saat dikirim atau disimpan sesuai Prosedur Klasifikasi, Penanganan Dan Pelabelan Informasi.

3.10.2 Ketentuan Penggunaan Akun Administratif atau Privileged

1. *User* ID dengan hak akses administrator harus memiliki *password* yang unik dan kuat.
2. *Password* dilarang dibagikan ke pihak lain, internal atau eksternal PT BPR BATU ARTOREJO.
3. Jika karyawan yang memiliki hak akses istimewa berhenti bekerja atau pindah posisi kerja maka *password* harus diubah pada hari yang sama. Dokumen perubahan hak akses harus disimpan.
4. Semua Pengguna harus mematuhi ketentuan menjaga Kerahasiaan *password* dan bertanggung jawab atas transaksi yang dilakukan menggunakan *User* ID & *password* mereka.
5. Hak akses administrator atau root hanya boleh digunakan dalam kondisi tertentu dan dilarang dipakai untuk kegiatan operasional sehari-hari.

3.10.3 Perubahan *Password* Default

1. *User* ID dan *password* default yang digunakan pada sistem, aplikasi atau perangkat jaringan harus segera diganti (reset) pada saat instalasi pertama. Karena *User* ID dan *password* default yang disediakan oleh produk atau vendor bisa mudah diketahui atau informasinya tersedia secara publik.
2. *User* ID dan *password* default yang tidak digunakan harus dinonaktifkan
3. *Password* default pada access points harus diubah setelah instalasi.

3.10.4 *User* Terkunci & Reset *Password*

1. Jika karyawan tidak dapat login ke sistem menggunakan *User* ID miliknya maka harus menghubungi Tim SMKI.
2. Setelah *User* ID dan *password* di reset, Pengguna harus segera mengubah *password* yang diberikan oleh sistem atau administrator saat login pertama kali.

3.10.5 Monitoring aktivitas Pengguna

1. Pengguna harus menyadari bahwa sesuai dengan prosedur keamanan informasi PT BPR BATU ARTOREJO, semua aktivitas Pengguna pada sistem akan dimonitor, dicatat dan diarsipkan. Jika diperlukan, catatan tersebut dapat digunakan sebagai bukti pelanggaran dan tindakan hukum sesuai ketentuan yang berlaku.
2. Seluruh aktivitas yang berpotensi membahayakan atau merusak aset informasi didefinisikan sebagai pelanggaran keamanan, seperti:
   a. Menghubungkan modem ke server tanpa persetujuan.
   b. Menyebarkan virus di jaringan.
   c. Mencuri data (*sniffing*) di jaringan.
   d. Percobaan menebak *password* milik pihak lain.
   e. Menghapus atau memodifikasi data tanpa ijin (ilegal).
   f. Mengunduh (download) atau mengirimkan konten yang berbahaya.
   g. Menjalankan tools pemindaian (*scan*) atau alat serangan komputer.
   h. Melewati atau membobol mekanisme pengendalian akses.
   i. Melakukan eksploit *vulnerability* pada sistem apa pun.
   j. Menginstal atau menggunakan *software* yang tidak berlisensi.
   k. Tindakan kriminal menggunakan komputer.

3.11 Ketentuan Keamanan Fisik dan Lingkungan (Aplikasi Internal)

3.11.1 Hak akses fisik

1. Tim SMKI harus menerapkan prinsip pemberian akses paling rendah ketika memberikan hak akses fisik kepada personel yang akan melakukan tugas atau pekerjaan di lokasi PT BPR BATU ARTOREJO.
2. Tim SMKI harus menerapkan pengendalian teknis, operasional, dan manajemen keamanan kepada seluruh personel yang membutuhkan akses fisik ke data, aplikasi, dan infrastruktur IT.
3. Kantor harus dilengkapi fasilitas kelistrikan yang memadai untuk menjaga kondisi listrik layanan Jaringan Bersama (Sharing Bandwitdh), seperti Stabilizer, Uninterrupted Power System (UPS) atau Generator Set dengan spesifikasi

kapasitas memadai dan harus dapat diaktifkan setelah hilangnya daya listrik dari PLN.

4. Alat pemadam kebakaran, seperti APAR harus terpasang dan diperiksa secara rutin. Semua personel harus dilatih untuk menggunakan alat pemadam kebakaran.

3.11.2 Pemantauan Aktivitas

1. Tim SMKI memiliki kamera CCTV untuk memonitor akses personel di ruang akses pemanfaatan data kependudukan Ditjen Dukcapil, Tim SMKI memantau CCTV dan merekam pada komputer / server dengan akses RAHASIA.
2. Semua kamera CCTV ditempatkan pada lokasi yang aman dan bersih (*clear*).
3. Aktivitas seluruh personel dan pengunjung harus dipantau dan direkam menggunakan CCTV saat masuk, berada dan keluar dari lokasi.
4. Semua kamera CCTV harus dilindungi dari ancaman gangguan atau penonaktifan.
5. Rekaman CCTV disimpan minimal selama 1 (satu) bulan.

3.12 Ketentuan Manajemen Risiko

3.12.1 Metodologi Penilaian Risiko

1. Metodologi penilaian risiko keamanan informasi, seperti Peraturan Otoritas Jasa Keuangan (POJK) Nomor 75 /POJK.03/2016 Tentang Standar Penyelenggaraan Teknologi Informasi Bagi Bank Perkreditan Rakyat Dan Bank Pembiayaan Rakyat Syariah, Surat Edaran Otoritas Jasa Keuangan Nomor 15/SEOJK.03/2017 tentang Standar Penyelenggaraan Teknologi Informasi bagi Bank Perkreditan Rakyat dan Bank Pembiayaan Rakyat Syariah, ISO 27005, Risk IT Framework bisa diikuti sebagai acuan dalam melaksanakan Penilaian Risiko Keamanan Informasi.
2. Penilaian Risiko Keamanan Informasi harus mencakup aset Jaringan Bersama (Sharing Bandwidth).
3. Penilaian Risiko Keamanan Informasi harus dilakukan secara berkelanjutan pada sistem, aplikasi atau aset informasi Jaringan Bersama (Sharing Bandwidth).

3.12.2 Identifikasi Aset

1. Semua aset informasi yang terkait dengan pemanfaatan data kependudukan Ditjen Dukcapil melalui layangan Jaringan Bersama (Sharing Bandwidth) harus diidentifikasi, didokumentasikan dan dikelola oleh Fungsi Manajemen Risiko dan Tim Teknologi Informasi atau Tim SMKI.
2. Aset informasi terdiri dari:
   a. Aset informasi elektronik, yaitu informasi dalam bentuk elektronik, seperti file database, data, dokumentasi sistem, Pedoman *atau user* manual, materi pelatihan, prosedur operasional, lisensi perangkat lunak, instalasi, rencana kesinambungan bisnis, kontrak, pedoman, data bisnis, dan lain-lain.
   b. Dokumen kertas (*hardcopy*), yaitu informasi dalam bentuk kertas fisik, seperti dokumen kontrak, laporan atau dokumentasi bisnis, dokumen pembelian, faktur, perjanjian lisensi dan lain-lain.
   c. Aset Sumber Daya Manusia, yaitu personel, pelanggan, vendor, tim keamanan dan lain-lain.
   d. Aset fisik, seperti aplikasi, perangkat jaringan, perangkat keamanan, media *backup*, printer, perangkat biometrik, rak server, PC dan lain-lain.
   e. Aset layanan, seperti layanan komputasi (*cloud*), jaringan, telekomunikasi, listrik, gas, air, pendingin udara, alarm penyusup, pengendalian kebakaran, generator dan UPS.
   f. Aset perangkat lunak, seperti aplikasi bisnis, perangkat lunak sistem, aplikasi manajemen pengetahuan, alat pengembangan, utilitas, dan lain-lain.

3.12.3 Identifikasi Risiko

1. Identifikasi risiko harus dilakukan berdasarkan informasi yang dikumpulkan pengguna utama dari setiap area proses bisnis.
2. Informasi identifikasi risiko dapat dikumpulkan dengan menggunakan:
   a. Kuesioner penilaian risiko.
   b. Wawancara dengan personel kunci.
   c. Diskusi kelompok.
   d. Tinjauan dokumentasi.

3. Penggunaan kuesioner adalah salah satu cara utama untuk melakukan pengumpulan data awal dalam proses penilaian risiko.
4. Ancaman (*threat*) terhadap aset informasi dapat didefinisikan sebagai peristiwa apa pun yang menyebabkan dampak kerugian, kerusakan atau hal lain yang tidak diinginkan PT BPR BATU ARTOREJO.
5. Sumber ancaman dapat berupa alam (banjir, kebakaran, badai), manusia (Pengguna, supplier, penyedia layanan pihak ketiga, kompetitor, *hacker*, dan pelanggan) dan teknis (*malware*).
6. Dalam menilai sumber ancaman, harus mempertimbangkan semua ancaman potensial yang dapat menyebabkan kerusakan pada aset informasi.
7. Kerentanan (*vulnerability*) pada aset informasi harus diidentifikasi. Tujuannya adalah untuk mendapatkan daftar kerentanan yang dapat dimanfaatkan (eksploitasi) oleh sumber ancaman potensial.
8. Kerentanan (*vulnerability*) pada aset informasi dapat bersifat teknis atau non-teknis.
9. Kerentanan (*vulnerability*) teknis terdapat pada *hardware*, *software* atau komponen teknologi lainnya yang digunakan oleh aset. Contoh kerentanan (*vulnerability*) teknis adalah bug pada *software*.
10. Kerentanan (*vulnerability*) non-teknis terdapat pada prosedural, administrasi dan lingkungan yang mengarah pada kemungkinan penyalahgunaan atau kerusakan aset.

3.12.4 Penanganan Risiko

1. Setelah risiko diidentifikasi dan dinilai, penanganan risiko dapat dikategorikan sebagai berikut:
   a. *Avoid* atau Penghindaran, yaitu menghilangkan, menarik diri dari atau tidak terlibat dari sumber ancaman.
   b. *Mitigasi* atau Pengurangan, yaitu mengurangi dampak atau kemungkinan ancaman.
   c. Transfer (*outsourcing* atau asuransi), yaitu menyerahkan kepada pihak ketiga untuk menanggung dampak atau kemungkinan ancaman.
   d. *Accept* atau Terima, yaitu menerima dampak atau kemungkinan ancaman.

2. Risiko yang berada di atas tingkat yang dapat diterima harus segera dilakukan penanganan risiko yang tepat. Penanganan risiko harus ditentukan dan disetujui oleh Direktur Utama atau Direktur Bidang Terkait. Penanganan risiko harus mempertimbangkan aspek bisnis, hukum, kebijakan dan peraturan yang berlaku.

3.12.5 Perhitungan Risiko Residual

1. Setelah menerapkan penangangan risiko maka risiko residual harus dihitung dan dianalisa apakah berjalan efektif serta menurunkan risiko pada area yang diterima (*risk acceptance*) oleh manajemen.
2. Risiko residual harus disetujui oleh Direktur Utama atau Direktur Bidang Terkait.

3.12.6 Pemantauan dan *Review* Berkala

1. Fungsi Manajemen Risiko dan Tim Teknologi Informasi atau Tim SMKI harus melakukan *review* secara rutin minimal 1 (satu) kali setiap tahun untuk memverifikasi kecukupan pengendalian risiko yang ada, risiko residual, dan tingkat risiko yang dapat diterima.
2. Fungsi Manajemen Risiko dan Tim Teknologi Informasi atau Tim SMKI dapat mengidentifikasi risiko baru yang timbul karena perubahan pada aset atau proses bisnis.
3. Fungsi Manajemen Risiko dan Tim Teknologi Informasi atau Tim SMKI menyimpan dokumentasi pengelolaan risiko.

3.13 Ketentuan Keamanan Jaringan

3.13.1 Persyaratan Keamanan Jaringan

Semua perangkat infrastruktur jaringan PT BPR BATU ARTOREJO harus mematuhi ketentuan keamanan sebagai berikut:

1. Tim SMKI bertanggung jawab atas penyediaan akses jaringan.
2. Daftar semua titik akses jaringan resmi (inventarisasi) dan justifikasi bisnis harus dicatat dan didokumentasikan.
3. Akses untuk menggunakan jaringan PT BPR BATU ARTOREJO harus mendapat persetujuan Tim SMKI.

3.13.2 Proses Pengamanan Jaringan

1. SMKI harus melakukan pemeriksaan jaringan secara rutin minimal setiap 1 (satu) bulan.
2. Tim SMKI harus membuat laporan pemeriksaan yang berisi daftar jaringan yang terdeteksi (resmi dan ilegal) serta lokasinya.
3. Tim SMKI harus melakukan investigasi apakah jaringan yang tidak sah (ilegal) dapat terhubung ke jaringan internal PT BPR BATU ARTOREJO atau melanggar ketentuan keamanan informasi.
4. Tim SMKI harus merujuk pada prosedur insiden keamanan jika menemukan jaringan tidak sah (ilegal) atau pelanggaran keamanan.

3.13.3 *Review* Pengendalian Jaringan

1. Tim SMKI harus me*review* pengendalian akses jaringan secara rutin minimal setiap 1 (satu) bulan.
2. Tim SMKI menyimpan dokumentasi pengendalian akses jaringan.

3.14 Ketentuan Keamanan Sumber Daya Manusia

3.14.1 Proses Seleksi Calon Karyawan (Rekrutmen)

1. Semua calon karyawan dan non karyawan (kontraktor atau vendor jika diperlukan) harus dilakukan proses seleksi (*screening*) sebelum bekerja di PT BPR BATU ARTOREJO.
2. Seleksi (*screening*) dilakukan sesuai kebijakan dan prosedur PT BPR BATU ARTOREJO dan wajib mematuhi undang-undang yang berlaku. Seleksi (*screening*) kurang lebih mencakup verifikasi:
   a. Identitas calon karyawan.
   b. Pendidikan, sertifikasi keterampilan dan pengalaman.
   c. Riwayat pekerjaan.
   d. Pemeriksaan catatan kriminal melalui SKCK (Surat Keterangan Catatan Kepolisian) sebagai tambahan untuk posisi atau jabatan tertentu.

3.14.2 Selama Bekerja

1. Semua personel harus menyetujui Pedoman, prosedur & petunjuk teknis keamanan informasi PT BPR BATU ARTOREJO. Persyaratan tersebut mencakup:
   a. Perjanjian Kerahasiaan atau *Non-Disclosure Agreement* (NDA).
   b. Tanggung jawab untuk menjaga aset perusahaan.
2. Unit Kerja Kantor Pusat yang Melakukan Fungsi SDM harus memastikan bahwa syarat dan ketentuan kerja disetujui oleh semua personel.
3. Unit Kerja Kantor Pusat yang Melakukan Fungsi SDM dan Tim SMKI harus memastikan bahwa semua personel mematuhi ketentuan keamanan sesuai dengan standar, pedoman, prosedur keamanan informasi dan petunjuk teknis keamanan informasi yang berlaku.

3.14.3 Perubahan (Mutasi) dan Pengakhiran Masa Kerja

1. Unit Kerja Kantor Pusat yang Melakukan Fungsi SDM dan atasan langsung personel yang mutasi atau berhenti bekerja harus memberi tahu personel tentang tanggung jawab keamanan informasi, yaitu:
   a. Persyaratan keamanan yang masih terikat termasuk keharusan untuk tidak mengungkapkan informasi RAHASIA.
   b. Tanggung jawab yang tercantum pada perjanjian Kerahasiaan atau *Non-Disclosure Agreement* (NDA).
   c. Seluruh Pedoman, standar atau kontrak lain yang masih terikat dan berlaku.
2. Ketika personel menerima tanggung jawab pekerjaan yang berbeda (mutasi) di PT BPR BATU ARTOREJO, atasan langsung personel saat ini harus memastikan bahwa aset informasi terkait akses data kependudukan Ditjen Dukcapil melalui Jaringan Bersama wajib diserahkan kepada Tim SMKI.
3. Tim SMKI harus memastikan bahwa akses ke sistem dan layanan jaringan Bersama yang dimiliki oleh personel yang mutasi atau berhenti telah dihapus atau dinonaktifkan.

3.15 Ketentuan Tindakan Korektif dan Preventif

1. Tindakan korektif, yaitu tindakan perbaikan untuk menghilangkan penyebab ketidaksesuaian dengan standar ISO 27001 dan prosedur keamanan informasi.

2. Tindakan preventif adalah tindakan perbaikan untuk mencegah potensi ketidaksesuaian atau yang tidak diinginkan dengan standar ISO 27001 dan prosedur keamanan informasi.
3. Ketidaksesuaian, yaitu kondisi yang tidak sesuai dengan persyaratan standar atau ketentuan yang berlaku, seperti ISO 27001, standar perjanjian tingkat layanan (SLA) atau kebijakan yang berlaku
4. Inisiator, yaitu personel (internal atau eksternal) yang melaporkan ketidaksesuaian.

3.15.1 Tindakan Koreksi dan Preventif Ketidaksesuaian

Ketidaksesuaian dapat terjadi karena beberapa hal berikut ini:

1. Sistem:
    1. Hasil pemeriksaan *vulnerability*, risiko dan pengujian penetrasi.
    2. Umpan balik dari audit internal dan eksternal.
    3. Hasil manajemen *review*.
    4. Persyaratan kebijakan dan regulasi yang berlaku.
2. Proses:
    5. Analisis laporan insiden.
    6. Perjanjian tingkat layanan (SLA)
    7. Pemantauan penggunaan sumber daya informasi.
    8. Event log, dll.
3. Perangkat keras, *software*, dan sistem terkait:
    9. Analisis masalah perangkat keras, *software*, dan sistem.

Semua karyawan didorong untuk melaporkan setiap ketidaksesuaian atau anomali dari penggunaan sumber daya informasi melalui prosedur manajemen insiden. Tindakan perbaikan preventif akan dilakukan setelah menerima laporan Ketidaksesuaian. Apabila ditemukan Ketidaksesuaian saat proses *review*, maka personel yang bertanggung jawab akan mencatat Ketidaksesuaian dalam bentuk Lembar Ketidaksesuaian Internal (*Non-Conformity Report* atau NCR).

1. Personel yang bertanggung jawab harus mengikuti prosedur yang diuraikan di bawah ini:
    10. Meninjau dan memverifikasi Ketidaksesuaian atau potensi Ketidaksesuaian

11. Menentukan penyebab utama Ketidaksesuaian.
12. Mengevaluasi dan merekomendasikan perbaikan untuk memastikan bahwa Ketidaksesuaian tidak muncul kembali (preventif).
13. Mencatat hasil rekomendasi yang diambil.

2. Ketua Tim SMKI bertanggung jawab untuk:
    14. Memverifikasi dan menyetujui tindakan perbaikan preventif yang diusulkan.
    15. Menugaskan personel untuk melaksanakan tindakan perbaikan preventif.
3. Personel yang bertanggung jawab melakukan perbaikan harus:
    16. Melakukan tindakan preventif dan korektif.
    17. Membuat dan menyimpan semua catatan tindakan perbaikan preventif.
    18. Membuat laporan rutin (bulanan) mengenai status Lembar Ketidaksesuaian Internal (NCR) ke Tim SMKI.
4. Tim SMKI bertanggung jawab akan meninjau status Lembar Ketidaksesuaian Internal (NCR), dan:
    19. Menganalisis laporan dan rencana perbaikan.
    20. Melakukan rapat dengan personel yang bertanggung jawab untuk me*review* dan menindaklanjuti masalah yang belum terselesaikan.
    21. Merekomendasikan tindak lanjut hasil *review* melalui audit internal (apabila diperlukan).

3.16 Ketentuan Internal Audit ISO 27001 SMKI

3.16.1 Perencanaan Audit

1. Koordinator Audit Internal akan menyiapkan rencana audit kepatuhan ISO 27001 SMKI berdasarkan analisa risiko dan kebutuhan PT BPR BATU ARTOREJO. Audit internal kepatuhan ISO 27001 harus dilaksanakan setidaknya 1 (satu) kali setiap tahun atau lebih jika diperlukan.
2. Rencana audit kepatuhan ISO 27001 SMKI harus mencakup:
    1) Tujuan dan ruang lingkup audit.
    2) Jadwal dan sumber daya yang diperlukan (biaya, peralatan, dll).
    3) Anggota tim audit.
    4) Pihak auditee dan lokasi audit.

3. Koordinator Audit Internal akan me*review*, memverifikasi dan mengkomunikasikan rencana audit kepatuhan ISO 27001 SMKI kepada semua pihak terkait (auditee).

3.16.2 Pelaksanaan Audit

1. Koordinator Audit Internal akan melakukan pertemuan pra-audit atau kickoff meeting dengan auditee. Tujuan pertemuan pra-audit atau kickoff meeting adalah:
   a) Untuk melakukan diskusi rencana dan ruang lingkup audit.
   b) Untuk memastikan tersedianya semua sumber daya (data, akses, dll) yang dibutuhkan dalam pelaksanaan audit
2. Pihak auditee akan menugaskan personel sebagai *counterpart* (pendamping) untuk memberikan data atau membantu Fungsi Audit Internal selama pelaksanaan audit.
3. Koordinator Audit Internal akan melakukan audit internal kepatuhan ISO 27001 SMKI menggunakan:
   a) Formulir Checklist kepatuhan ISO 27001 SMKI: berisi prosedur audit untuk masing-masing persyaratan ISO 27001 SMKI sesuai unit organisasi yang diaudit. Auditor yang ditugaskan bertanggung jawab mengisi dan memeriksa pemenuhan persyaratan ISO 27001 SMKI sesuai formulir ini.
   b) Standar ISO 27001 SMKI: berisi persyaratan ISO 27001 SMKI dan standar pengendalian keamanan.
4. Koordinator Audit Internal akan menjelaskan dan mengklarifikasi hasil observasi dan temuan kepada ketua tim dan seluruh tim auditor. Tim Fungsi Audit Internal harus memberikan bukti yang cukup memadai pada saat membahas (verifikasi) temuan.
5. Setelah pembahasan internal, Koordinator Audit Internal akan memaparkan hasil observasi dan temuan kepada seluruh pihak auditee terkait beserta bukti yang cukup.

3.16.3 Pelaporan Audit

1. Koordinator Audit Internal akan menyiapkan laporan audit berdasarkan pengamatan dan klarifikasi dari auditor. Temuan audit harus didukung oleh bukti

objektif. Koordinator Audit Internal mengkonsolidasikan semua temuan audit untuk penyusunan Laporan Audit.

2. Koordinator Audit Internal menerbitkan Lembar Ketidaksesuaian Internal (LKS) yang berisi ketidakesesuaian (*Non-Conformity Report*/NCR) formal kepada auditee untuk melaksanakan rekomendasi perbaikan yang diperlukan dan target tanggal penyelesaian perbaikan (preventif dan korektif) yang telah disetujui bersama auditee.
3. Koordinator Audit Internal akan me*review* dan mengirimkan LKS kepada pihak auditee. Tim SMKI akan melakukan follow-up setiap bulan mengenai status perbaikan atas temuan audit sesuai target tanggal penyelesaian perbaikan (preventif dan korektif) yang telah disepakati bersama auditee.

3.16.4 Tindakan Perbaikan (Remediasi) & Verifikasi

1. Koordinator Audit Internal harus melakukan monitoring tindakan perbaikan/remediasi (preventif dan korektif) sesuai yang tercantum pada Lembar Ketidaksesuaian Internal (*Non-Conformity Report*/NCR).
2. Koordinator Audit Internal harus memverifikasi bukti perbaikan/remediasi (preventif dan korektif) yang telah dilaksanakan oleh auditee.
3. Koordinator Audit Internal harus melakukan *update* Lembar Ketidakesesuaian Internal (NCR) jika tindakan perbaikan:
   a) Tidak diimplementasikan sesuai target tanggal yang disepakati.
   b) Hasil verifikasi menunjukan perbaikan tidak efektif.
4. Koordinator Audit Internal harus melakukan *update* status temuan menjadi *Closed* jika tindakan perbaikan yang dilakukan telah benar dan berjalan efektif.
5. Koordinator Audit Internal harus menjaga laporan dan catatan audit untuk audit kepatuhan ISO 27001 berikutnya.

3.17 Ketentuan Pelatihan dan Security Awareness

1. Tim SMKI harus mengadakan kegiatan pendidikan, pelatihan & sosialisasi keamanan informasi dalam Pemanfaatan Data Kependudukan Ditjen Dukcapil melalui Jaringan Bersama (Sharing Bandwidth) kepada seluruh personel untuk meningkatkan pemahaman pentingnya keamanan informasi.
2. Kegiatan pendidikan, pelatihan & sosialisasi harus:

a. Didukung oleh manajemen.
b. Memiliki tujuan yang jelas dan didokumentasikan.
c. Sebagai bagian dari program kesadaran keamanan informasi yang terus berlangsung.
d. Bertujuan untuk mengurangi risiko terjadinya insiden keamanan.

3. Semua personel harus diberi pelatihan dan pemahaman mengenai standar, pedoman, prosedur keamanan informasi dan petunjuk teknis keamanan informasi terkini sekurang kurangnya 1 (satu) tahun sekali.
4. Unit Kerja Kantor Pusat yang Melakukan Fungsi SDM dan Tim SMKI harus memasukkan program pelatihan dan kesadaran keamanan informasi pada saat orientasi karyawan baru. Materi pelatihan dan kesadaran keamanan informasi yang harus dibahas adalah kurang lebih mencakup:
   a. Keamanan informasi untuk data RAHASIA.
   b. Keamanan siber.
   c. Manajemen risiko keamanan informasi.
   d. Pelindungan data pribadi.
   e. Ancaman keamanan informasi.
   f. Standar, pedoman, prosedur dan petunjuk teknis keamanan informasi.
   g. Manajemen insiden keamanan informasi.
   h. Penggunaan informasi dan aset perusahaan secara tepat.
   i. Sanksi dan proses tindakan hukum jika melakukan pelanggaran.
4. Kegiatan pendidikan, pelatihan & sosialisasi keamanan informasi harus diberikan kepada seluruh karyawan agar:
   a. Memahami tujuan keamanan informasi, yaitu perlindungan aset informasi PT BPR BATU ARTOREJO terutama aspek Kerahasiaan (confidentiality), integritas (integrity) dan ketersediaan (availability).
   b. Memahami pentingnya menerapkan kebijakan, standar & prosedur keamanan informasi.
   c. Memahami tanggung jawab pribadi untuk keamanan informasi.
   d. Memastikan bahwa pengendalian keamanan informasi berfungsi secara efektif di lingkungannya.
5. Efektivitas pendidikan, pelatihan & sosialisasi keamanan informasi harus dinilai dan di-*review* melalui:

a. Mengukur tingkat pemahaman & kesadaran keamanan informasi yang ditunjukkan oleh peserta pasca mengikuti kegiatan ini.
b. Mengukur efektivitas kegiatan ini melalui frekuensi dan kehadiran peserta.

3.18 Ketentuan Pelaporan

1. Tim SMKI wajib membuat laporan bukti pelaksanaan implementasi SMKI ini dan mengirimkan ke DPP PERBARINDO, yaitu:
   a. Laporan Triwulanan yang dikirimkan pada tanggal 10 di bulan berikutnya. Contoh laporan triwulan 1 dikirimkan pada tanggal 10 April.
      1) Berita Acara Review User Jaringan Bersama (Sharing Bandwidth).
   b. Laporan Semesteran yang dikirimkan pada tanggal 10 di bulan berikutnya. Contoh laporan semester 1 dikirimkan pada tanggal 10 Juli.
      1) Laporan Kepatuhan Jaringan Bersama (Sharing Bandwidth).
   c. Laporan Tahunan yang dikirimkan pada tanggal 10 di bulan berikutnya. Contoh laporan tahunan 1 dikirimkan pada tanggal 10 Januari.
      1) Laporan Audit Internal Layanan Jaringan Bersama (Sharing Bandwidth) dalam bentuk lembar ketidaksesuaian internal (LKS).
      2) Laporan Tinjauan Manajemen.
      3) Daftar Risiko Layanan Jaringan Bersama (Sharing Bandwidth).
2. Format laporan diatas dapat diunduh pada link terlampir.
3. Kepatuhan mengirimkan laporan diatas akan menjadi penilaian untuk tergabung dalam ISO bersama PERBARINDO pada tahapan Surveillance ISO berikutnya.

BAB IV
PENUTUP

Petunjuk Teknis ini berlaku saat ditetapkan dan proses perubahan atau penyesuaian akan dilakukan secara berkesinambungan oleh Tim SMKI dengan memperhatikan regulasi dan kebutuhan bisnis PT BPR BATU ARTOREJO.

Untuk hal-hal yang belum tercantum dalam Petunjuk Teknis ini akan diatur dalam ketentuan tersendiri yang merupakan bagian tidak terpisahkan dari Ketentuan ini.

Implementasi Petunjuk Teknis ini akan dilakukan secara bertahap dengan memperhatikan kesiapan sistem, sumber daya, Kebijakan, Prosedur, dan kebutuhan bisnis.

RIWAYAT PERUBAHAN

Rev.	Tanggal	Bagian	Alasan Perubahan

A. TUJUAN :

Memastikan hanya dokumen SMKI khusus untuk data akses dukcapil beserta lampiran yang terkini dan sah tersedia di semua unit kerja yang memerlukan serta menetapkan penanganan dan pemeliharaan dokumen dan rekaman (bukti hasil) mulai dari penyimpanan, perlindungan, masa simpan sampai dengan pemusnahannya.

B. RUANG LINGKUP :

Penerbitan, revisi, pengesahan, pemberian identitas, dan pendistribusian dokumen data akses dukcapil. Penyimpanan, perlindungan, masa simpan bukti hasil sampai dengan pemusnahannya serta penanganan dokumen rahasia.

C. DEFINISI DAN KETENTUAN

- Dokumen adalah ketentuan tertulis yang digunakan secara resmi sebagai pedoman dalam penerapan SMKI pada organisasi.
- Dokumen Internal adalah Kebijakan, Pedoman, Standar operasional prosedur (SOP) dan dokumen lain disusun berdasarkan peraturan perundangan dan pedoman-pedoman eksternal yang berlaku yang diterapkan dilingkungan organisasi.
- Dokumen Eksternal adalah dokumen yang berasal dari luar organisasi yang dijadikan acuan untuk melakukan suatu pekerjaan atau kegiatan, Seperti undang-undang, Peraturan Pemerintah, Peraturan Daerah, *Manual Book*/Ketentuan/*Guidance*, dan lain-lain.
- Dokumen Induk adalah dokumen acuan yang memiliki beberapa turunan dokumen lainnya.

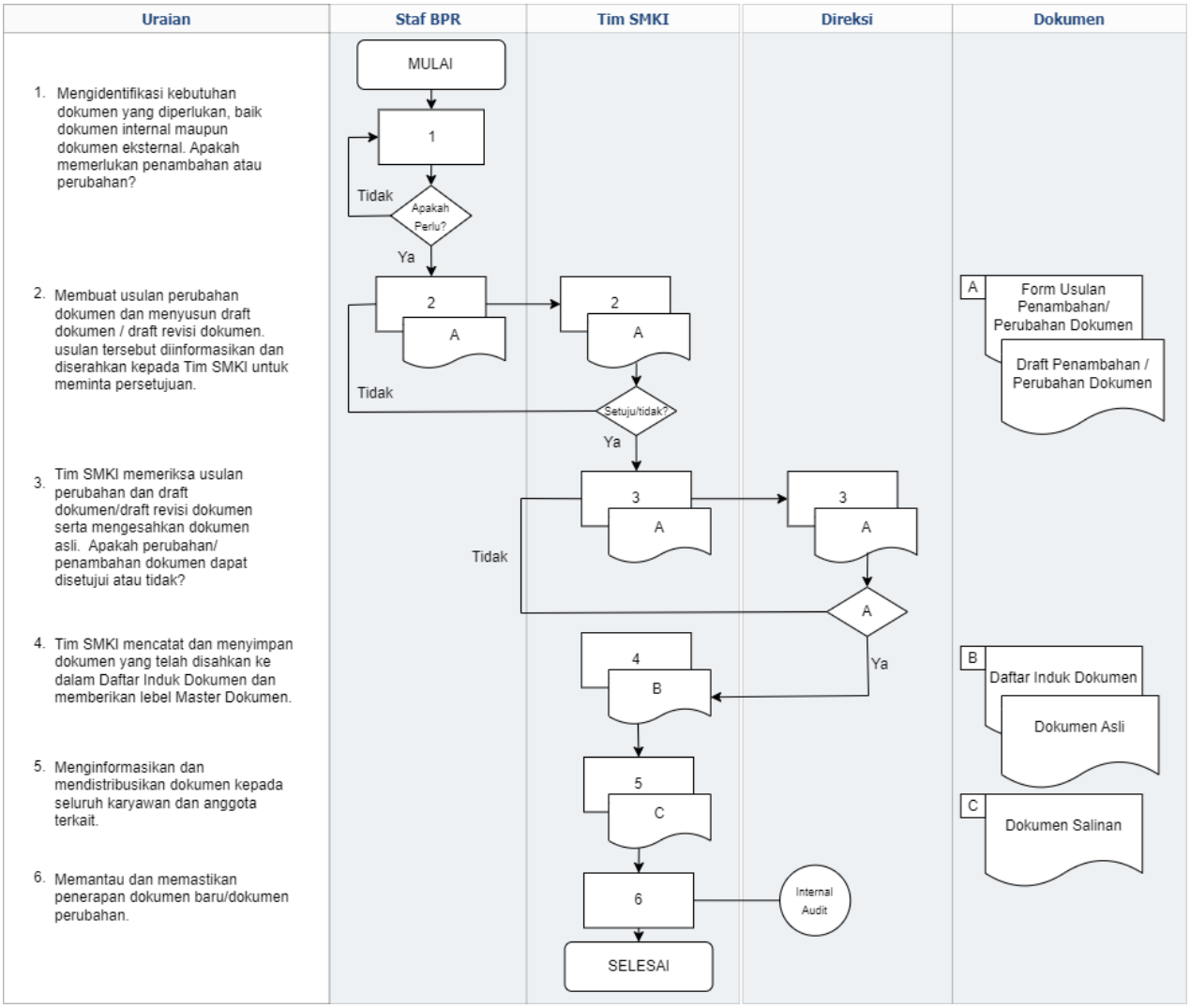
D. REFERENSI :

- SNI ISO/IEC 27001:2022
- Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi;
- Surat Edaran Dirjen Disdukcapil No. 400.8/11759/Dukcapil tanggal 8 Agustus 2023 tentang Tanggapan atas Surat Perbarindo Perihal ISO 27001.
- Surat Edaran Dirjen Disdukcapil No. 470/15017/Dukcapil tanggal 26 September 2022 tentang Perlindungan Data Kependudukan Dalam Keamanan Informasi.
- Surat Dirjen Dukcapil No. 470/17431/DUKCAPIL tanggal 24 September 2018 tentang Pemberitahuan Atas Konsep Sharing Bandwidth Komunikasi Data Perbarindo.
- POJK Republik Indonesia No. 8 Tahun 2023 tentang Penerapan Program Anti Pencucian Uang, Pencegahan Pendanaan Terorisme Dan Pencegahan Pendanaan Proliferasi Senjata Pemusnahan Massal di Sektor Jasa Keuangan.

E. PENANGGUNG JAWAB :

- Tim SMKI

F. ALUR PROSES



G. RINCIAN PROSEDUR :

- **PROSEDUR PENGENDALIAN DOKUMEN AKSES DUKCAPIL**

1. Penerbitan / Revisi Dokumen

   Identifikasi kebutuhan dokumen baru maupun penambahan/revisi dokumen SMKI dilakukan oleh Staf Bagian administrasi kredit dengan memberikan form usulan dengan melampirkan draft dokumen kepada Tim SMKI.

2. Pengesahan Dokumen

   Dokumen yang baru atau dokumen yang direvisi harus ditinjau kembali oleh Tim SMKI serta disetujui dan disahkan oleh Direksi dengan menandatangani kolom tanda-tangan yang disiapkan.

   - Pemberian Identitas BPR/BPRS

     Pemberian nomor dokumen yang sudah di berikan Perbarindo cukup ditambahkan kode sandi BPR/BPRS dari OJK.

     Maka penerapan di PT BPR Batu Artorejo menjadi : SOP.01.00/PND.01.00/PERB-SMKI/601786001/VIII/2023.

Kode	Uraian
PND	Panduan
SOP	Standar Operasional Prosedur
FR	Formulir
01	Urutan Dokumen
00	Urutan Revisi
PERB-SMKI	Tim SMKI Perbarindo
601786	Kode Sandi BPR
VIII	Bulan Terbit
2023	Tahun Terbit

     Note : Format Penomoran Dokumen dari perbarindo tidak boleh diubah oleh BPR/BPRS.

   - Pelabelan Dokumen

     Pelabelan dokumen ditetapkan menjadi 3 kategori yaitu: Master Dokumen, Salinan dokumen dan Obsolete.

1. Master Dokumen adalah Dokumen asli yang menjadi acuan pada setiap Salinan dokumen yang didistribusikan. Master dokumen dikendalikan oleh pengendali dokumen oleh Tim SMKI.
2. Salinan Dokumen adalah Dokumen yang didistribusikan.
3. Obsolete Dokumen adalah Dokumen yang sudah tidak digunakan dan didistribusikan.

KETERANGAN

1. NOMOR REVISI

- Dokumen yang pertama kali terbit diberi nomor 00. Selanjutnya jika terjadi revisi menjadi 01, 02 dan seterusnya hingga n. Jika terjadi perubahan nama dokumen maka diterbitkan edisi baru.
- Daftar induk dan distribusi dokumen serta status revisinya dicatat dalam form pemantauan dokumentasi.

2. DISTRIBUSI DOKUMEN

- Tim SMKI mendistribusikan dokumen kepada Staf BPR/BPRS dengan identitas nomor salinan sesuai yang tercantum dalam Daftar Induk dan Distribusi Dokumen dengan mengisi formulir Distribusi Dokumen.
- Distribusi untuk Perbarindo/pihak lain menggunakan Surat Pengantar.
- Staf BPR/BPRS tidak diizinkan untuk menggandakan dan mendistribusikan dokumen SMKI yang diterimanya tanpa persetujuan Direksi.
- Pencatatan pada form pemantauan dokumentasi.

3. PENYIMPANAN DAN PEMUSNAHAN DOKUMEN

- Setiap penerima dokumen wajib menyimpan, menjaga dan memelihara dokumen tersebut dengan sebaik-baiknya dan harus tersedia apabila dibutuhkan.
- Tim SMKI menyimpan master dokumen.
- Pencatatan pada form pemantauan dokumentasi

4. **DOKUMEN YANG SUDAH TIDAK BERLAKU**

Setiap dokumen yang sudah tidak berlaku wajib ditarik dan dimusnahkan sesuai ketentuan masa retensi oleh Tim SMKI dan disetujui Direksi. Pelaksanaan pemusnahan dokumen dicatat pada form pemantauan dokumentasi.

5. **MASA SIMPAN DOKUMEN**

Masa simpan dokumen di PT BPR Batu Artorejo diatur berdasarkan kategori sebagai berikut :

- Dokumen SMKI terkait data akses dukcapil dikategorikan sebagai dokumen dengan masa simpan selama 5 (lima) tahun.

- **PROSEDUR PENGENDALIAN BUKTI HASIL**

1. Penyusun dokumen SMKI dibuat pemantauan dokumentasi dalam form yang memuat:

a. Jenis dokumen eksternal atau internal, jika eksternal dikendalikan dan segera diadaptasikan. Jika internal segera disosialisasikan.
b. Tipe dokumen berupa Panduan, Standar Operasional Prosedur (SOP), Instruksi Kerja, Form dan Rekaman.
c. Nama Dokumen
d. Agenda berupa revisi, penerbitan, pemusnahan, pengesahan, distribusi
e. Tanggal pelaksanaan agenda
f. Kerahasiaan dokumen, apakah bersifat rahasia atau tidak
g. Masa Simpan
h. Penanggung jawab dokumen

2. Dokumen disimpan oleh Tim SMKI, di tempat yang terlindung agar terhindar dari kerusakan, kehilangan serta mudah diakses apabila diperlukan.

3. Pemusnahan Bukti hasil setelah memenuhi masa simpan dokumen dan harus mendapatkan persetujuan Direksi dengan menggunakan form pemantauan dokumentasi.

H. Dokumen terkait

1. Form Pengendalian Dokumen FR.01.00/PND.01.00/601786/VIII/2023
2. Form Usulan Revisi Dokumen FR.02.00/PND.01.00/601786/VIII/2023

3. Form Distribusi Dokumen FR.03.00/PND.01.00/601786/VIII/2023

Document Control	
Judul Dokumen	Manajemen Review ISO 27001 SMKI Semester 2 2023
No Document	FR.01.00/PND.01.00/PERB-SMKI/XI/2023
Versi Dokumen	-
Tanggal	

Dibuat oleh	Direview dan disetujui oleh:
	
PUSPITA RATNASARI	Wahyudin
Tim SMKI	Ketua SMKI