**PANDUAN SISTEM MANAJEMEN KEAMANAN INFORMASI**

**BANK XYZ**

****

**BANK XYZ**

**2022**

Panduan Sistem Manajemen Keamanan Informasi

Tanggal: 19 April 2022

Nomor: PM

Revisi: -

**PANDUAN SISTEM KEAMANAN INFORMASI**

**BANK XYZ**

Disahkan dan ditetapkan oleh

Direktur Utama PT Bank XYZ

Musa Alfonso

Daftar Isi

[1. Pendahuluan 5](#_Toc101296966)

[2. Konteks Organisasi 5](#_Toc101296967)

[2.1 Organisasi dan Konteks 5](#_Toc101296968)

[2.2 Kebutuhan dan Harapan 5](#_Toc101296969)

[2.3 Ruang Lingkup Penerapan SMKI 5](#_Toc101296970)

[2.4 Sistem Manajemen Keamanan Informasi 5](#_Toc101296971)

[3. Kepemimpinan 5](#_Toc101296972)

[3.1 Komitmen Manajemen 5](#_Toc101296973)

[3.2 Kebijakan 5](#_Toc101296974)

[3.3 Organisasi SMKI (Peran, Tanggung Jawab, dan Wewenang) 5](#_Toc101296975)

[4. Sasaran Keamanan Informasi 5](#_Toc101296976)

[5. Dukungan 5](#_Toc101296977)

[5.1 Sumber Daya 5](#_Toc101296978)

[5.2 Kompetensi dan Kepedulian 5](#_Toc101296979)

[5.3 Komunikasi 5](#_Toc101296980)

[5.4 Pengendalian Dokumen dan Rekaman 5](#_Toc101296981)

[6. Operasi 5](#_Toc101296982)

[6.1 Perencanaan dan Pengendalian Operasional 5](#_Toc101296983)

[6.2 Penilaian Risiko Keamanan Informasi 5](#_Toc101296984)

[6.3 Penanganan Risiko Keamanan Informasi 5](#_Toc101296985)

[7. Evaluasi Kinerja 5](#_Toc101296986)

[7.1 Pemantauan, Pengukuran, Analisis, dan Evaluasi 5](#_Toc101296987)

[7.2 Audit Internal 5](#_Toc101296988)

[7.3 Kaji Ulang Manajemen 5](#_Toc101296989)

[8. Perbaikan 5](#_Toc101296990)

[8.1 Ketidaksesuaian dan Tindakan Korektif 6](#_Toc101296991)

[8.2 Perbaikan Berkelanjutan 6](#_Toc101296992)

**PANDUAN SISTEM MANAJEMEN KEAMANAN INFORMASI**

**BANK XYZ**

# Pendahuluan

# Konteks Organisasi

## 2.1 Organisasi dan Konteks

## 2.2 Kebutuhan dan Harapan

## 2.3 Ruang Lingkup Penerapan SMKI

## 2.4 Sistem Manajemen Keamanan Informasi

# Kepemimpinan

## 3.1 Komitmen Manajemen

## 3.2 Kebijakan

## 3.3 Organisasi SMKI (Peran, Tanggung Jawab, dan Wewenang)

# Sasaran Keamanan Informasi

# Dukungan

## 5.1 Sumber Daya

## 5.2 Kompetensi dan Kepedulian

## 5.3 Komunikasi

## 5.4 Pengendalian Dokumen dan Rekaman

# Operasi

## 6.1 Perencanaan dan Pengendalian Operasional

## 6.2 Penilaian Risiko Keamanan Informasi

## 6.3 Penanganan Risiko Keamanan Informasi

# Evaluasi Kinerja

## 7.1 Pemantauan, Pengukuran, Analisis, dan Evaluasi

## 7.2 Audit Internal

## 7.3 Kaji Ulang Manajemen

# Perbaikan

## 8.1 Ketidaksesuaian dan Tindakan Korektif

## 8.2 Perbaikan Berkelanjutan

4.1 (pernyataan mengenai organisasi dan konteksnya)

|  |  |  |  |
| --- | --- | --- | --- |
| No | Issue | Internal | Eksternal |
| 1 | Pencurian Saldo nasabah | Lemahnya internal control |  |
| Masalah SDM |  |
| 2 | Penipuan yang mengatas namakan pihak bank |  | 1. Phising : Tindakan memperoleh informasi pribadi seperti user id, nomor rekening bank/no kartu kredit secara tidak sah 2. tidak peduli dengan keamanan data pribadi |
| 3 | Peraturan perundangan yang berlaku |  | Ketaatan terhadap peraturan perundangan yang berlaku terkait layanan mobile banking |
| 4 | Layanan Prima | Memberikan layanan prima yang menggunakan teknologi IT |  |

4.2 (kebutuhan dan harapan pemangku kepentingan serta pemenuhan perundangan) -- *ambil dari tugas*

Para pemangku kepentingan di dalam penerapan SMKI Bank XYZ sesuai dengan tabel di dibawah.

|  |  |  |  |
| --- | --- | --- | --- |
| *No* | *Pemangku Kepentingan* | *Harapan* | *Kebutuhan* |
| *1* | *Nasabah* | *Aplikasi aman namun mudah digunakan* | *Transaksi keuangan* |
| *2* | *Bank/ Organisasi Financial lain* | *Transaksi antar bank lancar dan aman* | *Transaksi keuangan lintas bank* |
| *3* | *Developer aplikasi* | *Aplikasi dapat berjalan dengan baik tanpa error* | *Membuat aplikasi dengan mudah* |
| *4* | *Tim infrastruktur*  *TI* | *Infrastruktur dapat memfasilitasi semua permintaan trafik aplikasi* | *Menyediakan infrastruktur untuk mendukung kinerja aplikasi* |
| *5* | *Infrastruktur TI external (AWS)* | *Infrastruktur outsourcing dapat memfasilitasi semua permintaan trafik aplikasi yang diminta* | *Menyediakan infrastruktur tambahan untuk mendukung kinerja aplikasi* |

4.3 (ruang lingkup penerapan SMKI) -- *ambil dari tugas*

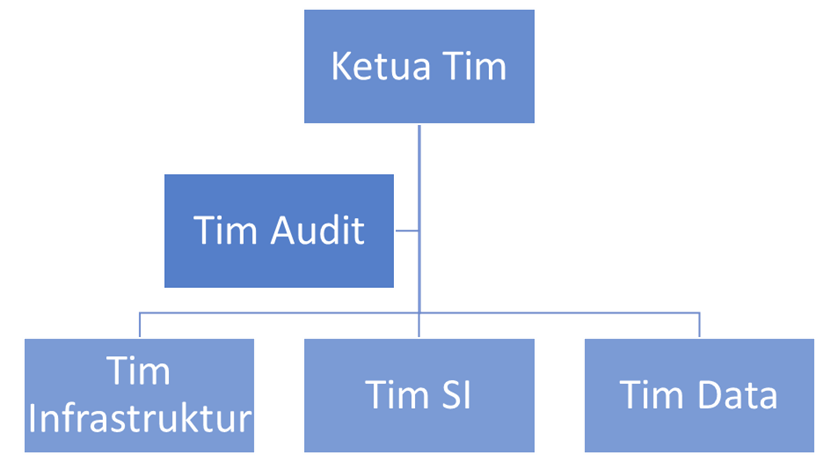
4.4 (pernyataan SMKI)

5. Kepemimpinan

5.1 (komitmen manajemen terhadap penerapan SMKI)

5.2 (kebijakan keamanan informasi) --  *ambil dari tugas*

5.3 (organisasi SMKI) -- *ambil dari tugas*

**

|  |  |  |
| --- | --- | --- |
| ***No*** | ***Peran*** | ***Tanggung Jawab*** |
| *1.* | *Ketua Tim* | 1. *Memberikan arahan dan masukan terkait penerapan SMKI* 2. *Menyediakan sumber daya bagi penerapan SMKI dalam layanan mobile banking* |
| *2.* | *Tim Audit* | *Melakukan audit TIK terhadap layanan mobile banking* |
| *3.* | *Tim Infrastruktur* | 1. *Mengembangakan infrastruktur yang mendukung layanan mobile banking* 2. *Melakukan pemeliharaan infrastruktur* |
| *4.* | *Tim SI* | 1. *Mengembangkan aplikasi mobile banking* 2. *Melakukan maintenance aplikasi* |
| *5.* | *Tim Data* | *Mengelola data transaksi dan pelanggan* |

6. Perencanaan

6.1 (identifikasi risiko dan rencana penanganannya) – *ambil dari tugas risk register*

6.2 (sasaran keamanan informasi) *-- ambil dari tugas*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Sasaran** | **KPI** | **Aktifitas pencapaian Kinerja** | **Indikator Pencapaian** | **Kebutuhan Sumber Daya** | **PIC** | **Jangka Waktu** | **Evaluasi** |
| 1 | Kebijakan penerapan keamanan pada layanan mobile banking | Kebijakan penerapan SMKI | Penyusunan kebijakan dan dokumentasi | Sertifikasi ISO 27001 | Seluruh organisasi | Ketua Tim | 1 Tahun | Sertifikasi |
| Pelaksanaan kegiatan operasional sesuai dengan prosedur |
| 2 | Pelanggan memahami prosedur keamanan penggunaan mobile banking | Kesalahan transkasi pelanggan | Menyusun media campaign untuk prosedur terkait | Kesalahan transkasi < 5% | Pelanggan, Tim SI, Tim Layanan Pelanggan | Ketua Tim | 1 Tahun | Laporan per triwulan |
| Membuat double authentication pada transaksi pelanggan |
| Membuat beberapa proses pengamanan (otomatis logout, permintaan perubahan password berjangka) |
| 3 | Manajamen keamanan sistem yang handal | Percobaan pelanggaran hak akses | Pengujian sistem | Keberhasilan pelanggaran hak akses < 0,5% | Tim SI, Tim Infrastruktur, Tim Data | Ketua Tim | 1 Tahun | Laporan per triwulan |
| Menyusun prosedur layanan keamanan |
| 4 | Kinerja sistem yang handal | Kinerja mobile banking | Audit TIK | Kinerja sistem > 99 % | Seluruh organisasi | Tim Audit | 1 Tahun | Laporan hasil audit |

7. Dukungan

7.1 (sumber daya) – identifikasi ketersediaan seluruh sumber daya yang ada (finansial, anggaran, infrastruktur, sdm, dll)

7.2 (kompetensi) – identifikasi ketersediaan sumber daya yang kompeten, dan pastikan adanya dukungan pelatihan untuk memenuhi kebutuhan kompetensi – *ambil dari tugas*

7.3 (kepedulian) – identifikasi rencana dan langkah-langkah peningkatan kepedulian SMKI di organisasi – *ambil dari tugas*

7.4 (komunikasi) – identifikasi bentuk komunikasi yang akan dilakukan saat peningkatan kepedulian serta bentuk komunikasi saat terjadi insiden keamanan informasi – *ambil dari tugas*

7.5 (pengendalian dokumen dan rekaman) – paparkan dan jelaskan bagaimana informasi terdokumentasi diatur dan dikendalikan (disimpan, dijaga, dipelihara) oleh organisasi – *ambil dari tugas*

8. Operasi

9. Evaluasi Kinerja

10. Perbaikan