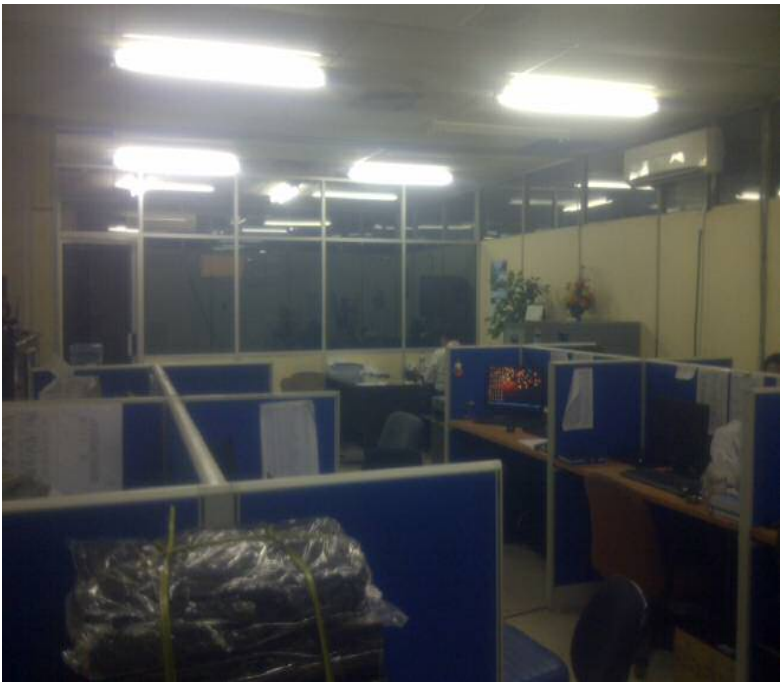
LAMPIRAN

LAMPIRAN

1. Ruangan Sub Divisi Sub Divisi Pengembangan Teknologi Informasi

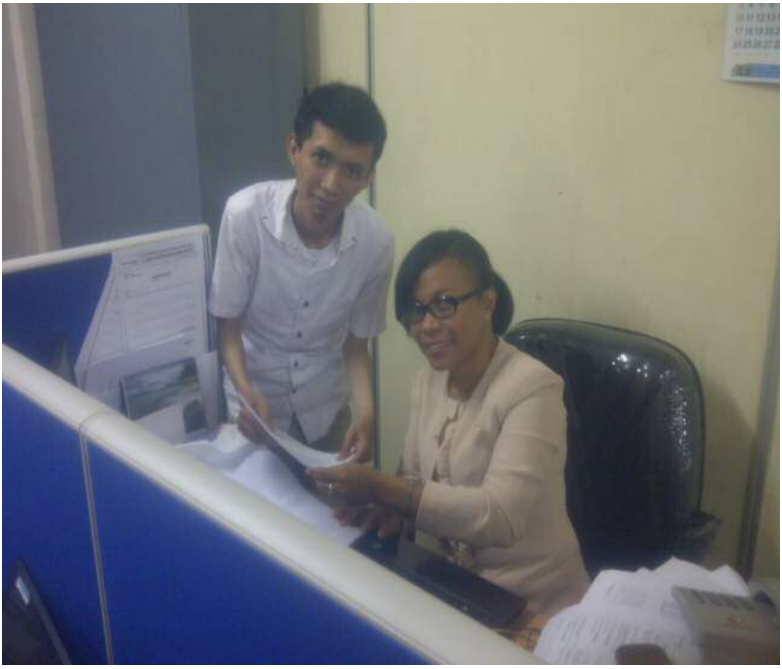


2. Depan Pintu Divisi Pengendalian Keuangan Dan Teknologi

3. NMS (Network Manage Security)

4. Dengan Kepala Sub Divisi Sub Divisi Pengembangan Teknologi Informasi

5. Lagi Bertanya Kepada Pegawai Sub Divisi Pengembangan Teknologi Informasi



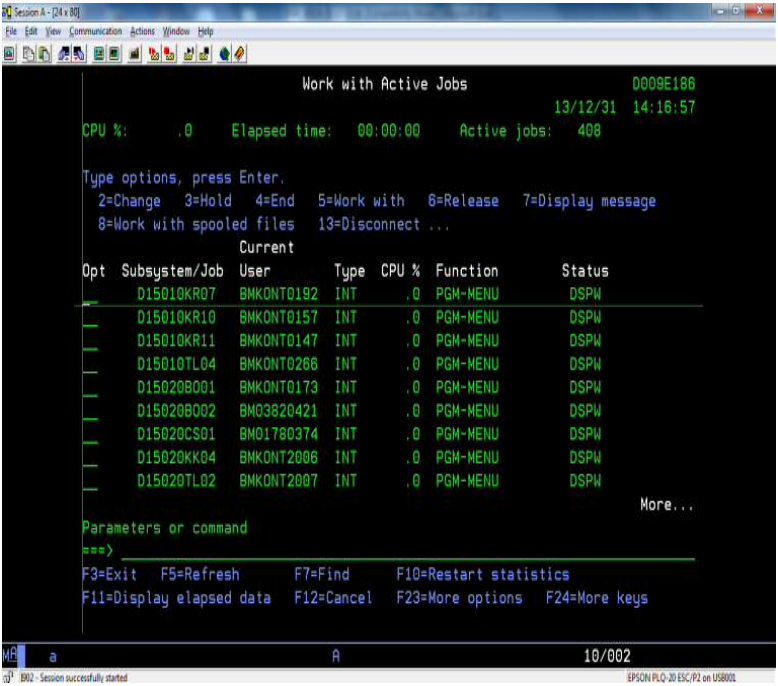
6. Photo Dari Lantai 2, Dibawah Lantai 1 Ruangan Teller

7. Photo Ruangan Teller, Tempat Antrian Nasabah

8. Pohoto Sistem Log In Aplikasi Core Banking

9. Pohoto Tampilan Menu Utama Aplikasi Core Banking Pada Divisi TI

10. Pohoto Log Pengguna



BANK XYZ	KEBIJAKAN DAN PROSEDUR PENGGUNAAN TEKNOLOGI INFORMASI BIDANG PENGAMANAN INFORMASI	SK. DIREKSI NO : DIR/13/KP Tgl 24 Februari 2009	BUKU V	HAL 11

11. Perlindungan terhadap Virus

11.1 Tujuan

Meminimalkan risiko dari infeksi virus terhadap sumber daya informasi perusahaan.

11.2 Pernyataan Pedoman

Software untuk perlindungan terhadap virus harus digunakan secara rutin guna melindungi aset komputasi perusahaan dari kerusakan yang dapat ditimbulkan oleh virus.

11.3 Standar

1. *Software* Anti Virus
   - Semua PC dan device electronic lainnya dilingkungan perusahaan dan / atau terhubung ke aset perusahaan harus dilindungi *software* anti virus.
   - *Software* anti virus harus diinstall pada semua :
     Server dan Microcomputer (PC, Laptop, dan electronic device lainnya) baik yang stand alone maupun yang dihubungkan ke jaringan komputer; baik di lokasi perusahaan maupun di lokasi lain tempat digunakannya perangkat keras tersebut.
   - *Software* anti virus harus selalu di *update* dengan versi terbaru, terutama *virus definition*-nya.

a. Apabila *Personil Computer* (PC) *users* yang digunakan terhubung ke jaringan, harus diupayakan adanya pemutakhiran secara otomatis dan efisien sehingga tidak menyita waktu dan tenaga kerja Unit Dukungan Teknis (*Technical Support)* disamping kebijakan ini dijalankan.

b. Apabila *Personil Computer* (PC) *users* merupakan *stand alone* unit, maka penanggung jawab aset berkewajiban untuk memutakhirkan antivirus yang dipakai secara berkala. Unit Dukungan Teknis *(Technical Support)* bertanggung jawab melakukan pengecekan secara periodik untuk memastikan hal ini dijalankan.

2. Scan Virus
   - *Server File* dan *Server* Aplikasi harus dikonfigurasikan sedemikian rupa sehingga *software* antivirus selalu aktif selama penggunaan komputer.
   - *Workstation*, perlu dikonfigurasikan sedemikian rupa secara otomatis melakukan *scanning file* yang hendak dibuka, dibaca atau setidaknya melakukan *scanning* ketika *start up*.
   - Semua *file* yang di *download* dari *internet* harus dilakukan *scanning* sebelum dapat digunakan.
   - Semua perangkat masukan portable (CD, *Diskette, Flash Disk / USB Drive*, dsb) harus dilakukan scanning sebelum dapat digunakan.
3. Pengecekan Terhadap Virus
   - Pada *microcomputer,* sudah diperbaiki.
   - Pada perangkat masukan *portable*, sebelum didistribusikan atau digunakan.
4. Pembasmian Virus
   - Untuk *user* yang terhubung ke *server*, scanning dilakukan secara otomatis.

- Untuk PC stand alone dilakukan oleh *user* sendiri, namun apabila kesulitan, dibantu oleh *Technical Support*.

5. Back-up *File*

   Semua *file* yang digunakan dan perlu diarsip, perlu di-*Backup* secara periodikal.

6. Program yang dapat merusak
7. *User* tidak boleh menulis, mengcopy, mendistribusikan atau menjalankan program yang dapat menimbulkan kerusakan / kerugian pada sistem komputer perusahaan.
   - Semua program yang dibuat sendiri dan yang dibuat oleh pihak ketiga harus mendapatkan izin dari *Board Of Director* sebelum dapat di-install pada PC *User*.
   - Penggunaan unauthorized / untrusted *software* yang merupakan tanggung jawab individu *user*s yang menjalankan / menggunakannya sehingga dapat dikenai sanksi apabila terbukti merusak aset perusahaan.

11.4 Tanggung Jawab

a. *Board Of Director*
   - Memastikan *software* antivirus yang digunakan mempunyai lisensi.
   - Mengadakan versi terbaru *software* antivirus.

b. Unit Dukungan Teknis (*Technical Support*)
   - Meng-install *software* antivirus, termasuk versi terbaru.
   - Mendistribusikan *software* antivirus ke seluruh lokasi operasional perusahaan.

c. *User*
   - Melakukan scanning pada semua *file* dan disket sebelum digunakan. Memberitahukan kepada *Security Administrator System* tentang keberadaan virus, baik yang terdeteksi maupun yang dicurigai.

BANK XYZ	KEBIJAKAN DAN PROSEDUR PENGGUNAAN TEKNOLOGI INFORMASI BIDANG JARINGAN KOMUNIKASI	SK. DIREKSI NO : DIR/13/KP Tgl 24 Februari 2009	BUKU IV	HAL 31

12. Pengendalian Akses

Pengendalian akses di jaringan komunikasi sangat penting dan harus diperhatikan karena jaringan komunikasi merupakan pintu utama untuk masuk ke dalam sistem informasi Bank. Jika tidak dikelola dengan baik, maka keamanan informasi menjadi terancam. Dalam menerapkan pengendalian akses, terdapat beberapa hal yang harus diperhatikan oleh Bank, yaitu:

a. akses ke jaringan komunikasi oleh user didasarkan pada kebutuhan bisnis dengan memperhatikan aspek keamanan informasi.
b. melakukan pemisahan jaringan komunikasi berdasarkan segmen baik secara logical maupun fisik, misalnya pemisahan antara lingkungan pengembangan dan produksi.
c. jika pemisahan secara fisik tidak dapat dilakukan, maka Bank harus memisahkan jaringan komunikasi secara logical dan memantau security access di jaringan komunikasi.
d. keputusan untuk terhubung ke jaringan komunikasi di luar Bank harus sesuai dengan persyaratan pengamanan dan secara formal disetujui oleh manajemen sebelum pelaksanaan.

e. menerapkan pengendalian yang dapat membatasi network traffic yang tidak sah atau tidak diharapkan.
f. konfigurasi perangkat jaringan komunikasi harus diset dengan baik. Fungsi-fungsi atau services yang tidak dibutuhkan harus dinonaktifkan.
g. penggunaan perangkat pengamanan jaringan komunikasi, seperti firewall, Intrusion Detection System (IDS), dan Intrusion Prevention System (IPS).
h. penggunaan penambahan perangkat monitor jaringan komunikasi (network management system) dengan memperhatikan pengamanannya.

pengujian secara berkala terhadap keamanan jaringan komunikasi, misalnya dengan penetration testing.

13. Renstra TI 2009-2013

Sasaran Rencana Strategis Teknologi Informasi

Penyusunan rencana strategis teknologi informasi ini memiliki sasaran yang memberikan kontribusi kepada PT. Bank XYZ sebagai berikut :

1. memiliki dasar dan arah pembangunan teknologi informasi dan komunikasi;
2. memiliki arsitektur teknologi informasi dan komunikasi yang didefinisikan untuk lima tahun ke depan;
3. memiliki standar pemilihan teknologi informasi dan komunikasi;
4. memiliki standar pengoperasian teknologi informasi dan komunikasi yang memperhatikan teknologi informasi dan komunikasi berdasarkan aspek keamanan/*security*, *scalability, availability, manageability* dan *performance*.

14. Prosedur Pengamanan Informasi

14.1. Prosedur Pengelolaan Aset

a. aset Bank yang terkait dengan informasi harus diidentifikasikan, ditentukan pemilik/ penanggungjawabnya dan dicatat agar dapat dilindungi secara tepat;
b. aset yang terkait dengan informasi tersebut dapat berupa data (baik *hardcopy* maupun *softcopy*), perangkat lunak, perangkat keras, jaringan, peralatan pendukung (misalnya sumber daya listrik, AC) dan sumber daya manusia (termasuk kualifikasi dan ketrampilan);
c. informasi perlu diklasifikasikan agar dapat dilakukan pengamanan yang memadai sesuai dengan klasifikasinya. Contoh dari klasifikasi tersebut adalah informasi ”rahasia” (misalnya data simpanan nasabah, data pribadi nasabah), ”internal” (misalnya peraturan tentang gaji pegawai Bank) dan ”biasa” (misalnya informasi tentang produk perbankan yang ditawarkan ke masyarakat). Klasifikasi dapat dibuat berdasarkan nilai, sensitivitas, hukum/ketentuan dan tingkat kepentingan bagi Bank.

14.2. Prosedur Pengelolaan Sumber Daya Manusia

a. sumber daya manusia baik pegawai Bank, konsultan, pegawai honorer dan pegawai pihak penyedia jasa yang memiliki akses terhadap informasi harus memahami tanggung jawabnya terhadap pengamanan informasi;
b. peran dan tanggung jawab sumber daya manusia baik pegawai Bank,

konsultan, pegawai honorer dan pegawai pihak penyedia jasa yang memiliki akses terhadap informasi harus didefinisikan dan didokumentasikan sesuai dengan kebijakan pengamanan informasi;

c. dalam perjanjian atau kontrak dengan pegawai Bank, konsultan, pegawai honorer dan pegawai pihak penyedia jasa harus tercantum ketentuan-ketentuan mengenai pengamanan Teknologi Informasi yang sesuai dengan kebijakan pengamanan informasi Bank. Sebagai contoh adalah perlu adanya klausula yang menyatakan bahwa mereka harus menjaga kerahasiaan informasi yang diperolehnya sesuai dengan klasifikasi informasi;
d. selain perjanjian antara Bank dengan perusahaan penyedia jasa, semua pegawai perusahaan penyedia jasa tersebut yang ditugaskan di Bank harus menandatangani suatu perjanjian menjaga kerahasiaan informasi (*non-disclosure agreement*);
e. pelatihan dan/atau sosialisasi tentang pengamanan informasi harus diberikan kepada pegawai Bank, konsultan, pegawai honorer dan pegawai pihak penyedia jasa. Pelatihan dan/atau sosialisasi ini diberikan sesuai dengan peran dan tanggung jawab pegawai serta pihak penyedia jasa;
f. Bank harus menetapkan sanksi atas pelanggaran terhadap kebijakan pengamanan informasi;
g. Bank harus menetapkan prosedur yang mengatur tentang keharusan untuk mengembalikan aset dan pengubahan/penutupan hak akses pegawai Bank, konsultan, pegawai honorer dan pegawai pihak penyedia jasa yang disebabkan karena perubahan tugas atau selesainya masa kerja atau kontrak.

BANK XYZ	KEBIJAKAN DAN PROSEDUR PENGGUNAAN TEKNOLOGI INFORMASI *BIDANG BUSINESS CONTINUITY PLAN*	SK. DIREKSI NO : DIR/13/KP Tgl 24 Februari 2009	BUKU VI	HAL 19

15. *Business Continuity Plan*

Kegiatan perbankan tidak dapat terhindar dari adanya gangguan/kerusakan yang disebabkan oleh alam maupun manusia misalnya terjadinya gempa bumi, bom, kebakaran, banjir, power failure, kesalahan teknis, kelalaian manusia, demo buruh, huru-hara dan sebagainya. Kerusakan yang terjadi tidak hanya berdampak pada kemampuan teknologi suatu Bank, tetapi juga berdampak pada kegiatan operasional bisnis Bank terutama pelayanan kepada nasabah. Bila tidak ditangani secara khusus, selain Bank akan menghadapi risiko operasional, juga akan mempengaruhi risiko reputasi dan berdampak pada menurunnya tingkat kepercayaan nasabah kepada Bank. Untuk meminimalisasi risiko tersebut, Bank diharapkan memiliki *Business Continuity Management* (BCM) yaitu proses manajemen terpadu dan menyeluruh untuk menjamin kegiatan operasional Bank tetap dapat berfungsi walaupun terdapat gangguan/bencana guna melindungi kepentingan para stakeholder. BCM merupakan bagian yang terintegrasi dengan kebijakan manajemen risiko Bank secara keseluruhan. BCM yang efektif perlu didukung dengan hal-hal sebagai berikut :

a. adanya pengawasan aktif manajemen;
b. melalui *Business Impact Analysis* dan *Risk Assessment;*
c. penyusunan *Business Continuity Plan* yang memadai*;*
d. dilakukannya pengujian terhadap BCP; dan

e. dilakukan pemeriksaan oleh Auditor Intern.

Business Continuity Plan (BCP) merupakan suatu dokumen tertulis yang memuat rangkaian kegiatan yang terencana dan terkoordinir mengenai langkah-langkah pengurangan risiko, penanganan dampak gangguan/bencana dan proses pemulihan agar kegiatan operasional Bank dan pelayanan kepada nasabah tetap dapat berjalan. Rencana tindak tertulis tersebut melibatkan seluruh sumber daya Teknologi Informasi (TI) termasuk sumber daya manusia yang mendukung fungsi bisnis dan kegiatan operasional yang kritikal bagi Bank.

Komponen prosedur BCP yang harus dimiliki Bank paling kurang meliputi *Disaster Recovery Plan* (DRP) dan Contingency Plan (CP). *Disaster Recovery* Plan (DRP) lebih menekankan pada aspek teknologi dengan fokus pada data recovery/restoration plan dan berfungsinya sistem aplikasi dan infrastruktur TI yang kritikal. Sedangkan *Contingency Plan* (CP) menekankan pada rencana tindak untuk menjaga kelangsungan bisnisnya apabila terjadi gangguan atau bencana termasuk tindakan antisipatif menghadapi kondisi terburuk misalnya bila TI yang digunakan sama sekali tidak dapat dipulihkan untuk waktu yang cukup lama. *Contingency Plan* (CP) harus meliputi pula rencana untuk memastikan kelangsungan seluruh pelayanan Bank termasuk yang dilaksanakan melalui *electronic banking*.

16. Internet dan Intranet

16.1. Tujuan

Mengatur dan mengawasi penggunaan *internet* / *intranet*.

16.2. Pernyataan Pedoman

User menggunakan *internet* / *intranet* hanya untuk hal-hal yang berkaitan dengan *user* tujuan bisnis perusahaan, serta sesuai dengan etika dan moral.

16.3. Standar

a. Aturan Penggunaan *Internet*
   - *User* bertanggung jawab terhadap perilaku dan kegiatannya selama menggunakan *internet*.
   - Menghindari akses ke *Website* yang tidak berkaitan dengan bisnis.
   - Menghindari *download file* yang besar.
   - Mematuhi perundang-undangan mengenai HAKI.
   - Melindungi informasi perusahaan dan klien (dengan cara menggunakan prosedur enkripsi, dsb).

b. Aturan Penggunaan *Intranet*
   - Akses *intranet* merupakan hak yang diberikan kepada *user* tertentu sesuai tugasnya.
   - *User* bertanggung jawab terhadap perilaku dan kegiatannya selama menggunakan *intranet*.

- Menghindari upload / *download file* yang besar.
- Mematuhi perundang-undangan mengenai HAKI.
- Melindungi informasi perusahaan dan klien (dengan cara menggunakan prosedur enkripsi, dsb).

c. Larangan Penggunaan *Internet*
   - Untuk hal-hal yang dapat merugikan perusahaan seperti mengungkapkan rahasia perusahaan dan klien dan / atau informasi sensitif. Melanggar kode etik dan moral, memicu persengketaan, dsb.
   - Untuk melakukan kegiatan yang dapat menimbulkan kerusakan pada sistem komputer / jaringan atau informasi yang ada pada sistem tersebut seperti menularkan virus, menimbulkan gangguan pada pelayanan jaringan, dsb.
   - Untuk mengirim *software* illegal, nomor kartu kredit illegal, *password* illegal, dsb.
   - Dengan cara menggunakan *workstation* aplikasi.

d. Larangan Penggunaan *Intranet*
   - Dengan cara menggunakan nama / *User ID user* lain.
   - Dengan cara melakukan bypass sistem pengamanan.
   - Untuk hal-hal yang dapat merugikan perusahaan seperti mengungkapkan rahasia perusahaan dan / atau informasi sensitif, memicu persengketaan, dsb.
   - Untuk melakukan kegiatan yang dapat menimbulkan kerusakan pada sistem komputer / jaringan atau informasi yang ada pada sistem tersebut seperti menularkan virus, menimbulkan gangguan pada pelayanan jaringan, dsb.
   - Menggunakan fasilitas *File* Transfer Protocol (FTP) untuk kepentingan pribadi.

- Untuk mengirim *software* illegal, nomor kartu kredit illegal, *password* illegal, dsb.

e. Pengawasan Penggunaan *Internet* / *Intranet*
   - *Website* Perusahaan
     a. Isinya dikelola oleh *Administrator Website* PT. Bank XYZ
     b. Perusahaan berhak mengumpulkan, memonitor, meng-copy, mentransmit, mencetak, dan menggunakan informasi yang masuk / keluar atau diproses melalui fasilitas *internet* / *intranet*.

f. Evaluasi Infrastruktur *Internet* / *Intranet*

   Evaluasi Infrastruktur *Internet* / *Intranet* dilakukan secara periodik oleh IT *Security Manager*.

g. Permintaan Akses ke *Internet* / *Intranet*

   Permintaan Akses ke *Internet* / *Intranet* diajukan tertulis pada *Manager* Unit Kerja ke *Board Of Director*.

h. Aplikasi melalui *Internet*
   - Dikembangkan dengan menggunakan *software* yang telah di-*approved* oleh *Board Of Director.*
   - Akses untuk informasi tertentu dibatasi dengan *User ID* / *password*.

16.4. Tanggung Jawab

a. *User*

   Melaporkan setiap pelanggaran pedoman ini, baik yang diketahui maupun dicurigai, kepada IT *Security Manager*.

b. Manajer Fungsi Terkait

Melaporkan kepada *Board Of Director* apabila terdapat pegawai yang melanggar pedoman ini, berganti posisi maupun berpindah tugas (mutasi), atau berhenti bekerja.

17. Prosedur Pengamanan Operasional Teknologi Informasi

Hal-hal yang harus diperhatikan dalam pengamanan operasional TI antara lain:

a. informasi dan perangkat lunak harus dibuatkan *backup* dan *prosedur recovery* yang teruji sesuai dengan tingkat kepentingannya;
b. Bank perlu mengantisipasi dan menerapkan pengendalian pengamanan yang memadai atas kelemahan sistem operasi, sistem aplikasi, *database* dan jaringan, termasuk ancaman dari pihak yang tidak berwenang seperti *virus, trojan horse, worms, spyware, Denial-Of-Service (DOS), war driving, , spoofing* dan *logic bomb*;
c. Bank harus memiliki kebijakan dan prosedur pengkinian anti-virus dan *patch* dan memastikan pelaksanaannya;
d. Bank harus membuat prosedur yang mencakup identifikasi *patch* yang ada, melakukan pengujian, dan menginstalasinya jika memang dibutuhkan;
e. Bank juga harus memelihara catatan dari versi perangkat lunak yang digunakan dan memantau secara rutin informasi tentang pengkinian (*enhancement*) produk, masalah keamanan, *patch* atau *upgrade*, atau permasalahan lain yang sesuai dengan versi perangkat lunak yang digunakan;
f. Bank harus menetapkan penggunaan enkripsi dengan menggunakan teknik kriptografi tertentu dalam mengamankan proses transmisi informasi yang sensitif, khususnya yang melalui jaringan di luar jaringan komunikasi Bank, sesuai dengan perkembangan teknologi terkini. Penggunaan teknik kriptografi

tersebut antara lain ditujukan untuk menjaga dan memastikan kerahasiaan (*confidentiality*), integritas (*integrity*), keaslian (*authenticity*), dan *non-repudiation*. Teknik yang dapat dipertimbangkan antara lain penggunaan enkripsi, *hash function*, dan *digital signatures* (menggunakan *Public Key Infrastructure);*

g. Bank harus menerapkan metode identifikasi dan otentikasi (*authentication*) sesuai tingkat pentingnya aplikasi misalnya penggunaan *one factor authentication* untuk aplikasi "biasa" serta penggunaan *two factor authentication* untuk aplikasi bersifat "kritikal";

h. Contoh metode identifikasi dan otentikasi antara lain *log on id* dan *password, token device* atau *biometrics* (misalnya *fingerprint, retina scan*, *face/iris/hand/palm analysis, signature recognition, voice recognition*);

i. Bank harus menyediakan dan melakukan kaji ulang atas jejak audit/*log* baik di tingkat jaringan, sistem maupun aplikasi serta menetapkan jenis *log* (misalnya *administrator log, user log, system log*), informasi yang harus dimasukkan ke dalam *log*, jangka waktu penyimpanan atau kapasitas *log* dengan memperhatikan ketentuan yang berlaku untuk keperluan penelusuran masalah.

BANK XYZ	KEBIJAKAN DAN PROSEDUR PENGGUNAAN TEKNOLOGI INFORMASI BIDANG PENGAMANAN INFORMASI	SK. DIREKSI NO : DIR/13/KP Tgl 24 Februari 2009	BUKU V	HAL 27

18. Password

1. Tujuan

Untuk memastikan bahwa *User* memahami tanggung jawab untuk melindungi hak akses yang telah diberikan dan dipercayakan.

2. Pernyataan Pedoman

a. perusahaan adalah organisasi pemberi jasa solusi TI terintegrasi yang meliputi, *software development*, ASP (Application Service Provider) dan *outsourcing data center* dan DRC sehingga sifat penyedia jasa adalah custodian yang menjaga kerahasiaan integritas dan ketersediaan data. Klien adalah pemilik data dan oleh karena itu bertanggung jawab penuh atas kepemilikan dan penggunaan data.

b. *Security Administrator System* wajib memberikan *User ID* dan *password* awal yang unik kepada setiap *User*, untuk akses ke sistem informasi perusahaan.

c. *User* bertanggung jawab atas semua kegiatan yang dilakukan di bawah *User ID*nya, termasuk aktivitas *Security Administrator System*.

d. *User* pengguna dalam organisasi harus menentukan *password* yang mudah diingat tetapi sulit untuk ditebak/diungkap.

3. Standar

a. *User ID*

Unik, bagi setiap *user* yang mengakses ke sistem komputer perusahaan guna menjamin akuntabilitas.

b. *Password*

Bersifat rahasia dan tidak boleh sama dengan *User ID*.

c. *Guest account*

- Diutamakan untuk dihapuskan atau dinonaktifkan;
- Apabila digunakan, maka passwordnya harus diganti;
- Hanya untuk kebutuhan pelatihan
- Akses dan penggunaanya sangat terbatas.
- Komposisi password

d. Komposisi *password*

- *Password* yang efektif

  Kombinasi huruf dan angka, contoh: HARI1N1.
  Akronim. Contoh: HARDIKNAS (Hari Pendidikan Nasional).

- *Password* yang tidak efektif

  Nama anggota keluarga, inisial, tanggal lahir anggota keluarga, alamat dan sebagainya.
  Pola yang mudah ditebak, seperti 1-2-3-4-5. 6666666,JUNI02
  Nama/istilah yang berkaitan/populer dengan perusahaan, jasa perusahaan dan industri perbankan

e. Perubahan *password*

- Harus dilakukan segera perubahan *password*

  Initial *Password*, bila diketahui atau dicurigai telah terjadi kebocoran dan bila menerima *User ID* baru (perubahan wewenang akses dan setelah aktivitas reset *password*)

- Secara perodikal

  Dilakukan oleh *user* dengan jangka waktu yag ditentukan oleh *Security Administrator System* dan *Security Administrator* Application. Bila tidak diubah dalam jangka waktu sebagaimana dimaksud *password* akan expired

- Ad-hoc (atas permintaan *User ID*)

  Apabila *user* lupa *password* mereka, maka *user* dapat meminta melalui permintaan tertulis ke *System Administrator* dengan tembusan ke IT *Security Manager*Apabila dalam situasi mendesak *user* dapat meminta *password* baru melalui telepon dengan diikuti permintaan tertulis melalui email, fax. Hal ini hanya dapat dilakukan kepada *user*s bersifat data entry (low risk *user*)

f. Perubahan status pegawai

Apabila terjadi mutasi, pemutusan hubungan kerja, berhenti, cuti panjang, cuti tidak dibayar, sakit berkepanjangan, pendidikan ke luar negri dan sebaginya, harus dilaporkan segera kepada *Security Administrator* Application dan *Security Administrator System*.

g. Penyimpanan *password*

- Bila tersimpan di sistem komputer, harus dalam format ter-enskripsi.
- Tidak boleh dalam bentuk hard coded, atau embedded dalam software dan sebagainya.

- Tidak boleh disimpan pada tempat yang mudah diakses / dilihat oleh user lain.

h. Larangan meminjamkan *password*

- Tidak diizinkan meminjamkan dan/atau meminjam *password* kepada *user* lain.

i. Pelimpahan kewenangan

- Dapat dilakukan dalam hal terjadinya kebutuhan atas pelimpahan kuasa / wewenang dari satu user kepada user lain.
- Pelimpahan kuasa / wewenang harus menggunakan surat tugas resmi yang diketahui oleh atasan langsung dan Security Administrator System.
- Harus mengacu kepada prinsip-prinsip keamanan.

j. Permintaan untuk account dan *password*

- Semua perubahan wewenang akses maupun permintaan User ID baru diajukan kepada Security Administrator Application dan Security Administrator System.

4. Tanggung Jawab

a. *User*

Menjaga kerahasiaan *password*nya.

b. *Security Administrator*

Bertanggung jawab mengatur manajemen *user* dan pengaturan konfigurasi *password* untuk memastikan akuntabilitas dari *user*.

c. Manajemen

Mengevaluasi efektifitas implementasi dari kebijakan ini secara periodik (minimal 1 tahun sekali).

19. Prosedur Pengamanan Fisik dan Lingkungan

a. fasilitas pemrosesan informasi yang penting (misalnya *mainframe, server*, PC, perangkat jaringan aktif) juga harus diberikan pengamanan secara fisik dan lingkungan yang memadai untuk mencegah akses yang tidak terotorisasi, kerusakan serta gangguan lain;

b. pengamanan fisik dan lingkungan terhadap fasilitas pemrosesan informasi yang penting meliputi antara lain pembatas ruangan, pengendalian akses masuk (misalnya penggunaan *access control card*, PIN, *biometrics*), kelengkapan alat pengamanan di dalam ruangan (misalnya *alarm*, pendeteksi dan pemadam api, pengukur suhu dan kelembaban udara, *close-circuit* TV) serta pemeliharaan kebersihan ruangan dan peralatan (misalnya dari debu, rokok, makanan/minuman, barang mudah terbakar);

c. fasilitas pendukung seperti AC, sumber daya listrik, *fire alarm* harus dipastikan kapasitas dan ketersediaannya dalam mendukung operasional fasilitas pemrosesan informasi;

d. aset milik pihak penyedia jasa (seperti *server*, *switching tools*) harus diidentifikasikan secara jelas dan diberikan perlindungan yang memadai seperti misalnya dengan menerapkan pengamanan yang cukup, *dual control* atau menempatkan secara terpisah dari aset milik Bank;

e. Harus dilakukan pemeliharaan dan pemeriksaan secara berkala terhadap fasilitas pemrosesan informasi dan fasilitas pendukung sesuai dengan prosedur yang telah ditetapkan.

20. Prosedur Pengamanan Logic (Logical Security)

a. Bank harus memiliki prosedur formal (tertulis dan telah disetujui oleh manajemen) tentang pengadministrasian *user* yang meliputi pendaftaran, perubahan dan penghapusan *user*, baik untuk *user* internal Bank maupun *user* eksternal Bank (misalnya vendor atau pihak penyedia jasa);

b. Bank harus menetapkan prosedur pengendalian melalui pemberian *password* awal (*initial password*) kepada *user* dengan memperhatikan hal-hal sebagai berikut:
   - *password* awal harus diganti saat login pertama kali;
   - *password* awal diberikan secara aman, misalnya melalui amplop tertutup atau kertas berlapis dua;
   - password awal bersifat khusus (unique) untuk setiap user dan tidak mudah ditebak;
   - pemilik *user-id* terutama dari pegawai Bank, pegawai honorer dan pegawai pihak penyedia jasa harus menandatangani pernyataan tanggung jawab atau perjanjian penggunaan user-id dan password saat menerima *user-id dan password;*
   - *Password* standar (default password) yang dimiliki oleh sistem operasi, sistem aplikasi, *database management system*, dan perangkat jaringan harus diganti oleh Bank sebelum

diimplementasikan dan sedapat mungkin mengganti *user ID* standar dari sistem (default user ID).

c. Bank harus mewajibkan user untuk:
   - menjaga kerahasiaan password;
   - menghindari penulisan password di kertas dan tempat lain tanpa pengamanan yang memadai;
   - memilih password yang berkualitas yaitu:
     a. panjang *password* yang memadai sehingga tidak mudah ditebak;
     b. mudah diingat dan terdiri dari sekurang-kurangnya kombinasi 2 tipe karakter (huruf, angka atau karakter khusus);
     c. tidak didasarkan atas data pribadi user seperti nama, nomor telepon atau tanggal lahir;
     d. tidak menggunakan kata yang umum dan mudah ditebak oleh perangkat lunak (untuk menghindari *brute force attack*), misalnya kata '*pass*', '*password*', 'adm', atau kata umum di kamus;
   - mengubah password secara berkala;
   - menghindari penggunaan password yang sama secara berulang.

d. Bank harus menonaktifkan hak akses bila user id tidak digunakan pada waktu tertentu, menetapkan jumlah maksimal kegagalan password (failed login attempt) dan menonaktifkan password setelah mencapai jumlah maksimal kegagalan password;

e. Bank harus melakukan pemeriksaan/review berkala terhadap hak akses user untuk memastikan bahwa hak akses yang diberikan sesuai dengan wewenang yang diberikan.

f. Sistem operasi, sistem aplikasi, database, utility dan perangkat lainnya yang dimiliki oleh Bank sedapat mungkin membantu pelaksanaan pengamanan password, sebagai contoh:
   - memaksa user untuk mengubah passwordnya setelah jangka waktu

tertentu dan menolak bila user memasukkan password yang sama dengan yang digunakan sebelumnya saat mengganti password;
- menyimpan password secara aman (ter-enkripsi);
- memutuskan hubungan atau akses user jika tidak terdapat respon selama jangka waktu tertentu (session time-out);
- menonaktifkan atau menghapus hak akses user jika user tidak melakukan log-on melebihi jangka waktu tertentu (expiration interval), misalnya karena cuti, pindah bagian.

g. Bank harus memperhitungkan risiko dan menerapkan pengendalian pengamanan yang memadai dalam penggunaan perangkat mobile computing dan media penyimpan data seperti notebook, hand phone, personal digital assistance, flash disk, external hard disk, termasuk bila menggunakan wireless access atau wireless network;

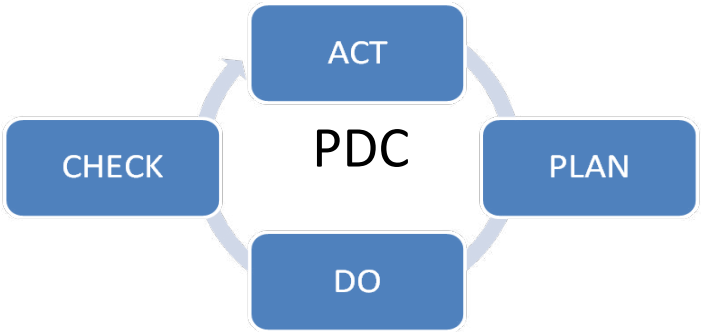
h. Bank harus memperhitungkan risiko dan menerapkan pengendalian pengamanan yang memadai terhadap titik akses (access point) ke dalam jaringan komputer dan/atau sarana pemrosesan informasi yang dapat dimanfaatkan oleh pihak yang tidak berwenang;

i. Bank yang menggunakan file sharing harus menetapkan pembatasan akses sekurang-kurangnya melalui penggunaan password dan pengaturan pihak yang berwenang melakukan akses;

j. Bank perlu memperhatikan proses security hardening terhadap perangkat keras dan perangkat lunak, seperti : setting parameter, patch.

BANK XYZ	KEBIJAKAN DAN PROSEDUR PENGGUNAAN TEKNOLOGI INFORMASI BIDANG PENGAMANAN INFORMASI	SK. DIREKSI NO : DIR/13/KP Tgl 24 Februari 2009	BUKU V	HAL 36

21. Kebijakan Pengamanan Informasi



Gambar 5.1 Siklus Plan, Do, Check, Act

21.1. Tujuan

Untuk memberikan panduan atau acuan bagi fungsi-fungsi dalam organisasi dalam menentukan dan menyusun aturan dan prosedur keamanan tekno*log*i informasi yang penerapannya dilakukan baik internal organisasi maupun di tempat klien mulai dari perencanaan, pengembangan, pemeliharaan, implementasi sistem dan dukungan pelayanan (service *support*).

21.2. Pernyataan Pedoman

Plan:

Untuk kebijakan *security*, sasaran, proses dan prosedur yang terkait untuk mengelola risiko dan *improvement security* dan hasilnya sesuai dengan kebijakan dan sasaran organisasi secara keseluruhan.

a. Eksekutif

Menentukan kebijakan organisasi terkait keamanan tekno*log*i informasi yang terintegrasi dengan kebijakan organisasi secara keseluruhan dan melakukan kaji ulang (review) paling tidak 1 (satu) tahun. Peran ini dibawakan langsung oleh pemimpin tertinggi organisasi yaitu Direktur Utama.

b. IT Security Manager

Adalah fungsi yang ditunjuk untuk menangani pengamanan TI secara keseluruhan dimulai dari penyusunan petunjuk pengamanan, memberikan masukan secara rutin kepada Dirut tentang perbaikan dan perubahan yang perlu dilakukan sehubungan dengan penerapan TI dalam operasional perusahaan, menelaah risiko dan bekerjasama dengan segala pihak termasuk vendor dalam rangka memberdayakan manajemen risiko terhadap sistem yang berjalan.

Do:

Mengimplementasikan dan mengoperasikan Kebijakan *Security*, pengendalian, proses dan prosedur.

a. Fungsi pengembangan

Mengimplementasikan kebijakan dan prosedur keamanan yang dilakukan oleh *System* Designer dalam merancang dan

mengembangkan sistem yang dari awal dapat diukur bahwa sistem yang dirancang itu diharapkan aman dan sesuai dengan standar dan requirement pengamanan yang ditentukan.

b. Fungsi pemeliharaan

Memastikan kebijakan, prosedur dan requirement keamanan yang sudah ditentukan dan telah diimplementasikan oleh fungsi-fungsi dibawahnya seperti *System* Designer, Programmer baik internal organisasi maupun tempat klien serta aturan yang dikeluarkan tidak bertentangan dengan kebijakan yang telah diatur eksekutif atau Direktur Utama.

c. Fungsi implementasi

Memastikan kebijakan dan prosedur telah dilaksanakan oleh fungsi di bawahnya seperti *Project Manager*, Implementor baik internal perusahaan maupun di tempat klien dan aturan yang dikeluarkan tidak bertentangan dengan kebijakan yang telah diatur eksekutif atau Direktur Utama.

d. Fungsi *Data Center* dan *Disaster Recovery Center*

Memastikan kebijakan, prosedur dan requirement keamanan yang sudah ditentukan telah diimplementasikan oleh fungsi-fungsi di bawahnya seperti Ka. Unit DC dan DRC, Supervisor DC, Operator DC dan DRC, Administrasi dan Library, Communication dan *System Support*, Fungsi Terkait, Klien, Tamu pada saat akses masuk ke *Data Center* maupun *Disaster Recovery Center* dan aturan yang dikeluarkan tidak bertentangan dengan kebijakan yang telah diatur Eksekutif atau Direktur Utama.

e. *Project Leader*

Memastikan adanya pedoman penggunaan keamanan dalam proyek yang dikembangkan dan tidak bertentangan dengan requirement dan ketentuan yang sudah ada.

f. Fungsi *Support*ing

Fungsi tersebut antara lain Financial *Accounting*, *General* Affair, Personil dan Legal melaksanakan kebijakan dan prosedur yang sudah ditentukan dalam aktivitas pengoperasian tekno*log*i informasi dalam organisasi.

g. *System supplier*

Adalah pihak terkait yang berperan merancang dan mengembangkan *System* dari awal dapat diukur bahwa sistem yang dirancang sesuai dengan kebutuhan dan requirement dan standar pengamanan yang ada.

Check:

Menilai apakah kebijakan dan prosedur konsisten diimplementasikan atau diaplikasikan dengan sesuai, mengukur unjuk kerja proses dibandingkan dengan Kebijakan *Security*, sasaran dan *best practice* dan hasilnya ke manajemen untuk dikaji ulang.

a. Internal audit

Melaksanakan penilaian terkait implementasi kebijakan dan prosedur paling tidak 1 (satu) kali dalam setahun dan frekwensinya ditambah bila diperlukan dimana hasilnya akan disampaikan ke manajemen untuk ditinjau (Management Review).

b. Fungsi Terkait

Fungsi terkait dengan pelaksanaan kebijakan dan prosedur keamanan merekam dan mendokumentasikan setiap risiko yang akan timbul serta

penyimpangan yang terjadi dalam form standar yang sudah ditentukan sebagai tindakan preventive.

Action:

Mengambil tindakan koreksi dan preventice berdasarkan hasil audit Kebijakan *Security* dan ditinjau manajemen atau informasi lain yang relevan untuk mencapai perbaikan yang berkesinambungan (continual *improvement*) terhadap Kebijakan *Security*.

a. IT *Security Manager*

   Merumuskan panduan keamanan informasi baru berdasarkan ketidaksesuaian hasil penerapannya dan hasil pelaksanaan audit.

b. Eksekutif (Direktur Utama)

   Menentukan kebijakan baru yang sudah dirumuskan IT *Security Manager* berdasarkan tindakan koreksi dari temuan audit dan ketidaksesuaian selama implementasi sebelumnya.

c. Fungsi terkait

   Fungsi pengembangan, fungsi pemeliharaan, fungsi Implementasi, Fungsi *Data Center* dan *Disaster Recovery Center*, *Project Leader*/*Project Manager*, Fungsi *Support*, *System Supplier* mengimplementasikan kebijakan baru dan diikuti dengan aturan-aturan terkait yang relevan dengan kebijakan baru yang sudah ditentukan.

BANK XYZ	KEBIJAKAN DAN PROSEDUR PENGGUNAAN TEKNOLOGI INFORMASI BIDANG PENGAMANAN INFORMASI	SK. DIREKSI NO : DIR/13/KP Tgl 24 Februari 2009	BUKU V	HAL 41

22. Laptop dan Komputer

22.1. Tujuan

Untuk mengendalikan pemakaian laptop atau portable komputer oleh personel yang diberikan tanggung jawab untuk memakainya agar dipergunakan sesuai dengan asas manfaat dan ketentuan yang berlaku.

22.2. Pernyataan Pedoman

a. *Board Of Director* mengeluarkan kebijakan terkait personel yang diberikan wewenang untuk menggunakan laptop.
b. Laptop merupakan aset perusahaan yang dipergunakan oleh personel yang diberikan wewenang untuk memakainya.
c. Manajemen melalui fungsi terkait menentukan standar pengendalian laptop.
   - Setiap pembelian laptop harus mempertimbangkan : dasar pembelian, *specification hardware* / software, lisensi, cost pada form yang sudah ditentukan.
   - Setiap penyimpanan laptop harus mempertimbangkan dan melakukan : identifikasi dan dicatat, disimpan ditempat yang sesuai, *log* history dan perbaikan.

- Setiap peminjaman dan perbaikan harus diajukan ke *General Affair* dan mengisi form peminjaman / perbaikan dan mendapatkan persetujuan dari atasan terkait.
- Setiap kehilangan harus dilaporkan ke *General Affair* dan personil legal dan dilengkapi dengan dokumen terkait (Berita Acara Kehilangan dari pihak berwajib di luar area kantor) utuk ditindaklanjuti.
- Stock taking minimal 1 (satu) kali dalam setahun.
- Setiap laptop harus dilengkapi dengan pengamanan tambahan.

d. Setiap laptop harus diinstall antivirus dan *software* lain dan setiap penambahan *software* harus seizin atasan dan *general affair*.
e. Semua data dan informasi adalah milik perusahaan yang diatur dalam ketentuan dan hanya dipergunakan untuk kepentingan perusahaan.
f. Pemakaian laptop pribadi harus mengikuti kebijakan yang sudah ditentukan.
g. Tidak boleh memberikan akses kepada pihak yang tidak berkepentingan.

BANK XYZ	KEBIJAKAN DAN PROSEDUR PENGGUNAAN TEKNOLOGI INFORMASI BIDANG PENGAMANAN INFORMASI	SK. DIREKSI NO : DIR/13/KP Tgl 24 Februari 2009	BUKU V	HAL 43

23. Kebijakan Pengamanan Perorangan

Standar

a. Umum

Label Klasifikasi Data; manajemen, terutama pemilik informasi, harus secara konsisten menerapkan standar klasifikasi data untuk memberikan identifikasi atau tanda bahwa informasi tersebut adalah rahasia. Label ini harus melekat kepada informasi rahasia tersebut dalam bentuk dan tekno*log*i yang sesuai. Contoh: label ini harus muncul di layar komputer ketika informasi rahasia ditampilkan, juga harus distempel di versi cetak dari informasi rahasia tersebut.

b. Khusus

- Pengungkapan Informasi Rahasia

Kebijakan dan prosedur harus disosialisasikan kepada personil dalam organisasi serta pihak ketiga yang terkait seperti auditor, dan memiliki kepentingan bisnis sah atas informasi ini.

Pengecualian tertulis harus ditentukan bila melibatkan kebijakan yang mengatur mengenai informasi rahasia yang terkait individu personil dalam organisasi.

Semua personil yang terlibat dalam kebijakan *security* harus menerima pernyataan kebijakan dan prosedur tertulis yang resmi dari PT. Bank XYZ mengenai pengelolaan informasi terkait individu personil tersebut.

Organisasi harus mengungkapkan adanya sistem yang menyimpan onformasi rahasia dan cara penggunaan informasi ini, dengan pengecualian terhadap personil yang terlibat dalam masalah hukum atau tindakan criminal.

- Mengelola permintaan Informasi Rahasia

Semua permintaan informasi yang berasal dari luar perusahaan dan bersifat rahasia (secret, confidential) berasal dari orang atau organisasi dialamatkan kepada IT *Security Manager*.

Semua permintaan informasi rahasia (secret, confidential) yang berada di luar proses bisnis normal dan yang berasal dari dalam perusahaan harus dialamatkan kepada IT *Security Manager*. Yang akan menentukan apakah informasi ini bisa diberikan atau tidak.

c. Pengelolaan Informasi Rahasia yang tepat

- Pengendalian informasi rahasia

Secara umum **PT. Bank XYZ** dapat mengumpulkan, memproses, menyimpan, mengirimkan dan menyebarkan informasi rahasia yang dibutuhkan untuk menjalankan fungsi secara layak. Contohnya: manajemen **PT. Bank XYZ** tidak boleh mengumpulkan aktivitas karyawannya di luar jam kerja terkecuali aktivitas ini berpengaruh terhadap kinerja pekerja dan reputasi yang tidak baik terhadap **PT. Bank XYZ.**

- Penghapusan Informasi Rahasia (Disposal)

Ketika informasi rahasia tidak lagi dibutuhkan, harus dirusakkan dengan mesin penghancur (shredder) atau dengan metode penghapusan informasi

lainnya yang disetujui oleh IT *Security Manager*. Penghapusan informasi rahasia di dalam disk komputer dan media magnetic lainnya harus dilaksanakan dengan cara penulisan tiban ulang. Pembuangan komputer dengan hard disk terpasang atau sistem penyimpan data lainnya harus diproses berdasarkan prosedur yang dikeluarkan oleh IT *Security Manager*.

- Pengalihan Informasi Rahasia

  Informasi rahasia tidak boleh dialihkan keluar dari **PT. Bank XYZ**. Izin untuk mengambil informasi keluar dapat diberikan oleh IT *Security Manager* atas persetujuan Direktur Utama. Perjanjian tertulis dari pihak ketiga (third-party non-disclosure agreements) mungkin dibutuhkan sebagai tambahan ketika informasi rahasia dialihkan dari kantor **PT. Bank XYZ**. Informasi rahasia tidak boleh dialihkan keluar wilayah Negara Republik Indonesia terkecuali ada izin tertulis dari IT *Security Manager* atas persetujuan Direktur Utama sepanjang tidak bertentangan dengan Undang-undang dan Peraturan yang berlaku.

- Mencegah pengungkapan yang tidak sengaja di layar

  Layar personal komputer, workstations, dan dumb terminals yang digunakan untuk memproses informasi sensitif atau data yang berharga, termasuk informasi rahasia, harus diposisikan sedemikian rupa sehingga tidak bisa begitu saja dilihat orang yang tidak berkepentingan.

d. Informasi Rahasia di dalam sistem komputer dan perangkat komunikasi

- Batasan kerahasiaan

  Semua pesanan yang dikirimkan melalui sistem komputer (*Internet*) dan komunikasi **PT. Bank XYZ** adalah milik dan property dari **PT. Bank XYZ**. Manajemen memiliki hak untuk memeriksa semua informasi yang disimpan dan ditransmisikan melalui sistem ini. Pemeriksaan semacam ini tidak

memerlukan persetujuan maupun Pengirim informasi. Karena sistem komputer dan komunikasi **PT. Bank XYZ** harus digunakan untuk tujuan bisnis perusahaan, maka karyawan diharapkan tidak memiliki kerahasiaan atas informasi yang mereka simpan, terima ataupun kirim melalui sistem ini.

- Pemeriksaan dari Informasi yang disimpan

  Setiap saat dan tanpa pemberitahuan terlebih dahulu, manajemen **PT. Bank XYZ** memiliki hak untuk memeriksa archived electronic mail, direktori *file* individu, *file* HDD dan informasi lainnya yang disimpan di dalam sistem informasi **PT. Bank XYZ**. Pemeriksaan semacam ini biasanya dilakukan untuk memastikan kepatuhan dengan kebijakan internal, mendukung proses investigasi internal dan sebagai bagian dan pengendalian manajemen **PT. Bank XYZ**.

- Peran Ka. Divisi dalam pengawasan

  Melakukan pengawasan langsung terhadap personil dibawahnya baik untuk tujuan kepatuhan terhadap kebijakan dan prosedur juga dalam proses investigasi, semua aktivitas pengawasan harus dicatat ke dalam *log* sebagai bahan tinjauan manajemen dan juga dapat menjadi dasar pengambilan tindakan pendisiplinan atau tindakan hukum.

- Merubah informasi yang disimpan di dalam sistem

  Manajemen memegang hak untuk menghapus, meringkas atau merubah informasi apapun yang disimpan di dalam sistem informasi dan komunikasi **PT. Bank XYZ**.

- Penggunaan rutin dari sistem *Backup*

  Semua *file* dan pesan yang disimpan di dalam sistem secara rutin disalin ke tape, disk, dan storage media lainnya. Hal ini berarti bahwa semua informasi yang disimpan di dalam sistem informasi perusahaan, meskipun telah

dihapus oleh karyawan yang bersangkutan, seringkali dapat dipulihkan dan dapat dipergunakan untuk keperluan pemeriksaan lebih lanjut oleh sistem *Administrator* ataupun petugas lainnya yang ditetapkan oleh manajemen.

BANK XYZ	KEBIJAKAN DAN PROSEDUR PENGGUNAAN TEKNOLOGI INFORMASI BIDANG JARINGAN KOMUNIKASI	SK. DIREKSI NO : DIR/13/KP Tgl 24 Februari 2009	BUKU IV	HAL 48

24. Kebijakan atas penggunaan layanan jaringan

Pengguna sebaiknya hanya diberikan akses ke layanan yang telah diijinkan. Suatu kebijakan sebaiknya diformulasikan terkait penggunaan jaringan dan layanan jaringan. Kebijakan ini meliputi :

a. jaringan dan layanan yang diijinkan untuk diakses;

b. prosedur otorisasi untuk menentukan siapa saja yang diijinkan untuk mengakses jaringan dan layanannya;

c. kontrol dan prosedur manajemen untuk melindungi akses ke sambungan jaringan dan layanannya;

d. media yang digunakan untuk mengakses jaringan dan layanannya (misalnya kondisi yang memungkinkan akses dial-up ke penyedia jasa Internet atau sistem remote).

Kebijakan penggunaan layanan pada jaringan sebaiknya konsisten dengan kebijakan kontrol akses bisnis.

Sambungan tanpa ijin dan tidak aman ke layanan jaringan dapat berpengaruh pada keseluruhan organisasi. Kontrol ini penting khususnya untuk hubungan jaringan ke aplikasi bisnis yang sensitif atau ke pengguna di lokasi yang beresiko tinggi, misalnya publik atau daerah eksternal yang berada di luar manajemen dan kontrol keamanan organisasi.

BANK XYZ	KEBIJAKAN DAN PROSEDUR PENGGUNAAN TEKNOLOGI INFORMASI BIDANG JARINGAN KOMUNIKASI	SK. DIREKSI NO : DIR/13/KP Tgl 24 Februari 2009	BUKU IV	HAL 49

25. Kebijakan dan Prosedur Pengamanan Jaringan Komunikasi

Tujuan kebijakan dan prosedur pengamanan jaringan komunikasi adalah untuk melindungi informasi dari pihak yang tidak berwenang dan kerusakan atau kerugian informasi karena akses yang tidak terkontrol. Berikut ini merupakan hal-hal yang sekurang-kurangnya terdapat pada kebijakan dan prosedur pengamanan jaringan :

a. Bank setidaknya harus memiliki *user management* yang mengatur level otorisasi setiap user.
b. Perjanjian kerahasiaan data/Non-Disclosure Agreements (NDA) diidentifiasikan dan diimplementasikan untuk menjamin keamanan informasi Bank. Setiap kontrak kerja yang dibuat oleh pihak bank, harus menerapkan perjanjian kerahasiaan tersebut.
c. Setiap risiko yang timbul akibat kerjasama dengan pihak ketiga merupakan tanggung jawab pihak manajemen. Karena itu segala macam bentuk kerja sama dengan pihak ketiga harus diidentifikasikan dan didefinisikan terlebih dahulu.
d. Secara rutin dilakukan evaluasi oleh pihak internal dan external pada jaringan komunikasi.

Secara detil masalah pengamanan informasi akan dibahas pada Buku 5 Pengamanan Informasi.

BANK XYZ	KEBIJAKAN DAN PROSEDUR PENGGUNAAN TEKNOLOGI INFORMASI BIDANG MANAJEMEN	SK. DIREKSI NO : DIR/13/KP Tgl 24 Februari 2009	BUKU I	HAL 50

26. Kepala Sub Divisi Pengembangan Teknologi Informasi

Berikut ini merupakan tanggung jawab yang dilaksanakan oleh Kepala Sub Divisi Arsitektur dan Implementasi Aplikasi yang sekurang-kurangnya sebagai berikut :

1. Menyusun konsep kebijaksanaan umum bidang arsitektur aplikasi dan Arsitektur infrrastruktur
2. Menyusun rencana kerja dan anggaran bidang arsitektur aplikasi dan Arsitektur infrrastruktur.
3. Melakukan analisis lingkungan untuk perencanaan arsitektur aplikasi core banking, supporting application (aplikasi pendukung), integration system (sistem integrasi), dan analytical application (sistem analisa), networking, security, data center, dan disaster recovery system;
4. Melakukan penelitian terhadap arsitektur aplikasi dan infrastruktur perbankan bekerja sama dengan divisi terkait;
5. Menciptakan/mengusulkan arsitektur aplikasi dan infrastruktur baru/penyempurnaan arsitektur aplikasi/infrastruktur;
6. Mengevaluasi tata kerja dalam upaya peningkatan pelayanan dan operasional bank;
7. Melakukan studi banding dengan bank lain atau institusi lain dalam rangka penyempurnaan arsitektur aplikasi/infrastruktur;;
8. Melakukan tugas pekerjaan lain yang diberikan oleh kepala divisi;

9. Melakukan koordinasi kerja dengan team di bawahnya yaitu team Core Banking Architecture, Supporting Application Architecture, Integration Architecture, Analytical Architecture, networking, security, data center, dan disaster recovery system;
10. Menyusun konsep kebijaksanaan umum bidang implementasi arsitektur aplikasi/infrastruktur;
11. Menyusun rencana kerja dan anggaran bidang implementasi arsitektur aplikasi/infrastruktur;
12. Melakukan analisis lingkungan untuk perencanaan implementasi aplikasi core banking, supporting application, integration system, dan analytical application, networking, security, data center, dan disaster recovery system;
13. Melakukan penelitian terhadap implementasi aplikasi/ infrastruktur perbankan bekerja sama dengan divisi terkait;
14. Menciptakan/mengusulkan implementasi aplikasi/ infrastruktur baru / penyempurnaannya;
15. Mengevaluasi tata kerja dalam upaya peningkatan pelayanan dan operasional bank;
16. Melakukan studi banding dengan bank lain atau institusi lain dalam rangka penyempurnaan proses implementasi aplikasi/infrastruktur;

27. BPP SDM

1. IKHTISAR JABATAN

Berperan secara aktif dalam teknis penyelenggaraan pendidikan dan latihan pegawai, assesment centre, ujian jabatan dan kegiatan pendidikan dan latihan lainnya.

3. TANGGUNG JAWAB PEKERJAAN

Bertanggung jawab atas pelaksanaan tugas dalam :

a. Mempersiapkan segala sesuatu dalam penyelenggaraan pendidikan dan latihan pegawai, antara lain :

- Menginventarisasi program/materi pendidikan dan latihan dalam penyelenggaraan pendidikan dan latihan;
- Menginventarisasi kebutuhan pelatihan dan pengembangan pegawai sesuai job spesifikasi;
- Menginventarisasi program pelatihan dan pengembangan yang telah dilaksanakan baik *on the job training* maupun *off the job training;*
- Mengkaji dan merumuskan jenis pelatihan serta pengembangan modul-modul pelatihan;
- Mengusulkan calon peserta pendidikan atau pelatihan;
- Mempersiapkan serta mengelola sarana dan prasarana pelatihan;
- Mempersiapkan tenaga pengajar pelatihan;
- Mempersiapkan absensi untuk pelatih maupun peserta pelatihan;

- Mempersiapkan honor untuk pelatih dan uang saku/uang jalan untuk peserta pelatihan;
- Menatausahakan dan mengevaluasi pelaksanaan pendidikan atau pelatihan.

	CONTINUITY PLAN	Tgl 24 Februari 2009		54

28. Penilaian Risiko

Penilaian risiko (*risk assessment*) yang terdiri dari identifikasi dan pengukuran risiko merupakan tahap kedua yang harus dilalui dalam penyusunan suatu BCP. Proses ini diperlukan untuk dapat mengetahui tingkat kemungkinan terjadi gangguan pada kegiatan bank yang penting (*critical*) serta dampaknya bagi kelangsungan usaha bank. *Risk assessment* sekurang-kurangnya mencakup hal-hal sebagai berikut:

a. Melakukan analisis atas dampak gangguan atau bencana terhadap bank, nasabah dan industri keuangan;
b. Melakukan *gap analysis* dengan membandingkan kondisi saat ini dengan langkah atau skenario yang seharusnya diterapkan;
c. Membuat peringkat potensi gangguan bisnis berdasarkan tingkat kerusakan (*severity*) dan kemungkinan terjadinya (*likelihood*).

29. Prosedur Penanganan Insiden dalam Pengamanan Informasi

Hal-hal yang harus diperhatikan Bank dalam melakukan penanganan insiden dalam pengamanan informasi antara lain:

a. insiden yang terjadi harus dapat diidentifikasi, dilaporkan, ditindaklanjuti, didokumentasikan dan dievaluasi untuk memastikan dilakukannya penanganan yang tepat dan untuk mencegah terulangnya insiden;
b. Bank harus menetapkan prosedur penanganan insiden yang mengatur antara lain:
   - Siapa yang harus melaporkan insiden;
   - Jenis insiden yang harus dilaporkan;
   - Alur pelaporan insiden (*point of contact*);
   - Siapa yang bertanggung jawab untuk menindaklanjuti insiden;
   - Analisis atas insiden untuk mencegah terulangnya insiden;
   - Pendokumentasian bukti terkait insiden dan tindak lanjutnya.
c. Bank perlu mempertimbangkan pembentukan tim khusus yang menangani insiden pengamanan (CSIRT – *Computer Security Incident Response Team* atau CERT – *Computer Emergency Response Team*) sesuai dengan skala usaha dan kompleksitas TI Bank;
d. Pegawai Bank, pegawai honorer dan pegawai pihak penyedia jasa diminta untuk melaporkan setiap kali menemukan indikasi atau potensi kelemahan pada sistem dan aplikasi sesuai kebijakan dan prosedur pelaporan insiden pengamanan. Kelemahan yang perlu dilaporkan misalnya adanya virus dari *e-mail* yang masuk.