DIKELUARKAN OLEH	TANGGAL	NOMOR	HALAMAN
KOMITE PENGELOLAAN RISIKO		**005/KPR/2017**	**1 / 122**

PERIHAL

KEBIJAKAN TATA KELOLA TEKNOLOGI INFORMASI

KEPUTUSAN

Surat Keputusan Kebijakan Tata Kelola Teknologi Informasi ini diterbitkan sebagai panduan dan arahan untuk dilaksanakan oleh PT Danareksa (Persero) dan Anak Perusahaan. Dengan diterbitkannya Kebijakan ini, maka Kebijakan sebelumnya yakni SK KPR No. 005/KPR/2007 bulan Mei 2007 perihal Kebijakan Teknologi Informasi menjadi tidak berlaku.

Selanjutnya, apabila di kemudian hari terbit peraturan yang lebih tinggi seperti Undang-Undang, regulasi pemerintah, atau regulasi internal yang menyebabkan satu atau beberapa aturan dalam Kebijakan ini menjadi tidak berlaku, maka yang harus diacu adalah peraturan yang lebih tinggi tersebut dan aturan yang tidak berlaku tersebut akan disesuaikan untuk mengacu kepada peraturan yang lebih tinggi tataran hukumnya.

PERSETUJUAN

Nama	Jabatan	Tanggal	Tanda Tangan
R.A.M. Irwan Satya Utama	Head Divisi Risk Management & SOP		
Bondan Pristiwandana	Direktur		
Marciano H. Herman	Direktur		
Hoesen	Direktur		
Heru D. Adhiningrat	Direktur Utama		

DAFTAR ISI

I. PENDAHULUAN

Latar Belakang

Teknologi informasi (TI) sangat besar manfaatnya dalam pengembangan usaha suatu perusahaan, sehingga perlu dikembangkan secara terarah dan terukur di PT Danareksa (Persero) dan Anak Perusahaan atau (yang selanjutnya disebut "**Danareksa**") guna mendukung strategi bisnis Danareksa sejalan dengan tujuan jangka panjang, menengah, dan jangka pendek yang ingin dicapai oleh Danareksa sebagai grup.

Agar teknologi informasi dapat dimanfaatkan secara optimal, terukur, terarah dan memenuhi prinsip-prinsip *Good Corporate Governance* (GCG), maka pemanfaatan dan pengembangan teknologi informasi di Danareksa harus berdasarkan pada suatu sistem tata kelola, termuat dalam sebuah *master plan*, dan dikembangkan secara bersinergi sesama entitas.

Berdasarkan pertimbangan sebagaimana dimaksud tersebut diatas, perlu menetapkan Kebijakan Tata Kelola Teknologi Informasi.

Maksud dan Tujuan

Kebijakan Tata Kelola Teknologi Informasi ini (selanjutnya disebut "**Kebijakan**") ditujukan untuk membuat suatu kerangka dan landasan implementasi yang dapat memberikan jaminan bagi Danareksa:

1. Mendukung strategi bisnis, baik jangka panjang, menengah maupun pendek.
2. Memenuhi prinsip GCG sehingga dapat dimanfaatkan secara optimal, terukur dan terarah.

Beberapa komponen lingkungan kerja terkait TI yang akan dibahas lebih lanjut adalah kebijakan strategis TI, pengelolaan layanan TI, pengelolaan keamanan TI, infrastruktur TI, manajemen kualitas layanan TI, manajemen kelangsungan usaha dan monitor & pengendalian internal. Tentunya untuk mencapai tujuan secara optimal dibutuhkan koordinasi segenap Unit Kerja Danareksa, kerja sama dari setiap pegawai Danareksa, dan dukungan teknologi sistem informasi yang memadai, baik perangkat keras maupun perangkat lunak yang mempertimbangkan aspek manfaat, efisiensi dan keamanan.

Penyusunan panduan ini bertujuan agar kebijakan TI dapat mendukung Tata Kelola Tl yang dapat menjaminkan bahwa:

1. TI selaras dengan kebutuhan bisnis;
2. TI dapat mendukung bisnis dan memberikan manfaat optimal;
3. Sumber daya TI digunakan dengan penuh tanggung jawab;

4. Risiko-risiko yang terdapat dalam TI dikelola dengan baik;
5. Kepatuhan terhadap aturan tata kelola yang ditetapkan; dan
6. Penerapan tata kelola TI merupakan tanggung jawab Direksi, dengan akuntabilitas pelaksanaan disepakati untuk diserahkan kepada salah satu direktur sesuai dengan kepentingan bisnis masing-masing entitas.

Kebijakan ini juga disusun dengan tujuan membentuk kesamaan sudut pandang dalam pengimplementasian pengelolaan dan keamanan TI. Kebijakan ini juga dimaksudkan untuk memberikan arahan dan petunjuk kepada seluruh *User* yang ada di Danareksa, sehubungan dengan keamanan yang dipandang dari sisi Premises dan *Information Technology*. Di dalam Kebijakan ini dijelaskan ketentuan-ketentuan pokok dan tata cara yang berlaku dan harus diikuti oleh seluruh *User* dalam lingkup Danareksa. Dalam pelaksanaannya, seluruh lingkup kegiatan di dalam Kebijakan ini dikoordinasikan oleh Divisi *Information Technology* (IT) PT Danareksa Sekuritas atau Entitas yang ditunjuk oleh Manajemen PT Danareksa (Persero), (yang selanjutnya disebut "**Divisi IT**")

Sebagai upaya untuk mendukung pelaksanaan pekerjaan, pemberian produk dan layanan, pelaksanaan kepatuhan dan pengamanan aset intelektual perusahaan, diperlukan suatu sistem yang akan sedapat mungkin mengurangi risiko operasional terkait dengan TI. Setiap gangguan yang berkenaan dengan aspek-aspek tersebut akan secara potensial mengurangi kinerja pegawai perusahaan dan mengurangi kemampuan untuk memberikan jasa dan layanan yang berkualitas, yang pada akhirnya memberikan pengaruh terhadap kinerja perusahaan. Oleh karena itu sudah menjadi tanggung jawab pihak perusahaan untuk dapat memberikan jaminan lingkungan kerja yang mendukung setiap pegawai untuk dapat melaksanakan tugas dan kewajibannya secara optimal serta memberikan layanan yang terbaik kepada para pelanggan dan pemangku kepentingan lainnya.

Kebijakan ini bersifat rahasia dan ditujukan hanya untuk penggunaan di lingkungan internal Danareksa. Kebijakan ini dapat diterbitkan dalam bentuk cetakan ataupun dalam media elektronik. Dilarang mengkopi sebagian maupun seluruh isi dari Kebijakan tersebut tanpa izin tertulis dari Direksi.

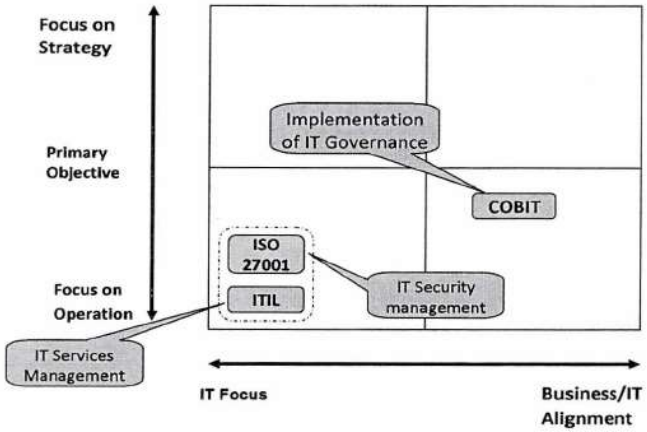
II. DASAR KEBIJAKAN

1. Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
2. Peraturan Menteri Badan Usaha Milik Negara Nomor PER-01/MBU/2011 tanggal 1 Agustus 2017 tentang Penerapan Tata Kelola Perusahaan yang Baik (*Good Corporate Governance*) pada Badan Usaha Milik Negara.

3. Peraturan Menteri Badan Usaha Milik Negara Nomor PER-02/MBU/2013 tanggal 18 Februari 2013 tentang Panduan Penyusunan Pengelolaan Teknologi Informasi Badan Usaha Milik Negara;
4. Peraturan Otoritas Jasa Keuangan Nomor 17/POJK.03/2014 tanggal 18 November 2014 tentang Penerapan Manajemen Risiko Terintegrasi bagi Konglomerasi Keuangan;
5. Peraturan Otoritas Jasa Keuangan Nomor 18/POJK.03/2014 tanggal 18 November 2014 tentang Penerapan Tata Kelola Terintegrasi bagi Konglomerasi Keuangan;
6. Surat Edaran Otoritas Jasa Keuangan Nomor 14/SEOJK.03/2015 tanggal 25 Mei 2015 tentang Penerapan Manajemen Risiko Terintegrasi bagi Konglomerasi Keuangan;
7. Surat Edaran Otoritas Jasa Keuangan Nomor 15/SEOJK.03/2015 tanggal 25 Mei 2015 tentang Penerapan Tata Kelola Terintegrasi bagi Konglomerasi Keuangan;
8. Keputusan Direksi PT Danareksa (Persero) nomor KD-38/032/RM-CS tanggal 1 Oktober 2014 tentang Kebijakan Sentralisasi dan Pemberdayaan Anak Perusahaan PT Danareksa (Persero) dan Anak Perusahaan;
9. Struktur Organisasi PT Danareksa (Persero).

III. REFERENSI *FRAMEWORK* TEKNOLOGI INFORMASI (TI)

Beberapa referensi IT *Governance* berdasarkan *best practices* dapat dilihat pada gambar berikut ini:



Gambar 1. *Framework* IT *Governance Best Practices*
Sumber: *Guide Share Europe*

Masing-masing *framework* diatas dapat diterapkan dalam situasi atau kondisi perusahaan yang berbeda-beda. Dalam penyusunan Kebijakan, sesuai dengan latar belakang bahwa IT

Governance sebagai parameter untuk menjamin keselarasan TI dengan tujuan bisnis korporasi dan kebijakan strategis maka dapat dilakukan pendekatan dengan menggunakan *framework* COBIT, ITIL, ISO 27001, TOGAF dan PMBOK dengan beberapa penyesuaian yang diperlukan.

Perbandingan IT *Governance Framework*

Ada beberapa IT *Governance framework* yang umum dipergunakan untuk implementasi tata kelola TI, antara lain:

a. *Control Objectives for Information and related Technology* (COBIT) yang dikembangkan oleh IT *Governance Institute* untuk membantu organisasi/perusahaan dalam melakukan penilaian tata kelola atas proses TI yang dimiliki.

b. *The* IT *Infrastructure Library* (ITIL) yang dikembangkan oleh *Office of Government Commerce* untuk membantu suatu organisasi/perusahaan dalam menyediakan tata kelola atas layanan operasional TI yang baik dan memenuhi harapan pengguna.

c. The ISO/IEC 27001:2005(150 27001) yang dikembangkan oleh ISO untuk membantu suatu organisasi/perusahaan dalam memastikan tata kelola dalam hal *Information Security Management System* (ISMS).

d. *The* ISO/IEC 38500:2008(ISO 38500) merupakan standar baru tentang tata kelola TI yang dikeluarkan oleh ISO untuk membantu suatu organisasi/perusahaan dalam menerapkan prinsip-prinsip yang harus dimiliki dalam tata kelola yang baik.

e. *The Open Group Architecture Framework* (TOGAF) yang dikembangkan oleh *The Open Group* untuk membantu organisasi/perusahaan dalam melakukan pengembangan suatu *Enterprise Architecture* guna menciptakan keunggulan kompetitif melalui TI *Project Management Body of Knowledge* (PMBOK) yang dikembangkan oleh *Project Management Institute, Inc*. (PMI) untuk membantu suatu organisasi/perusahaan dalam pengelolaan suatu *project*, program dan portfolio TI yang baik. Tabel dibawah merupakan ringkasan perbandingan IT *Governance Framework* berdasarkan faktor-faktor sebagai berikut:

   i. Cakupan proses, yaitu seberapa luas proses TI yang dicakup oleh *framework* dimaksud,
   ii. Kejelasan panduan, yaitu adanya penjelasan yang lengkap sampai dengan petunjuk penerapannya (*how to*) sehingga memudahkan pengguna dalam penerapannya.

Nama *Framework*	Cakupan Proses	Kejelasan Panduan	Penggunaan Secara Umum
COBIT	Mencakup semua proses tata kelola TI yang meliputi: a. Perencanaan dan pengorganisasian (PO); b. Akuisisi dan implementasi; c. Penyampaian dan dukungan; d. Pengawasan.	Penjelasan cukup sampai kepada kontrol-kontrol yang harus ada dan tidak sampai kepada petunjuk rinci penerapannya.	Sebagai referensi audit TI dan atau penilaian tata kelola TI.
ITIL	Proses manajemen layanan TI yang meliputi 5 tahapan siklus layanan (*service life cycle*): a. *Service strategy* b. *Service design* c. *Service transition* d. *Service operation* e. *Continual service improvement*	Penjelsan meliputi ke 5 tahapan *service life cycle* dan proses-proses pengelolaan layanan IT *Service Management* (ITSM) pada setiap tahapan *service life cycle*.	Sebagai penjelasan terhadap disiplin dan tanggung jawab dalam penentuan dan manajemen layanan TI yang efektif.
ISO 27001	Dokumen standar sistem manajemen keamanan informasi atau *Information Security Management System* (ISMS), yang memberikan cakupan proses untuk melakukan evaluasi, implementasi dan memelihara	Petunjuk untuk penerapan keamanan informasi sebgai penjagaan informasi dalam rangka memastikan kelangsungan bisnis, minimasi risiko bisnis dan mengoptimalkan peluang bisnis dan investasi.	Implemetasi terhadap ISMS

	keamanan informasi berdasarkan *best practice* dalam pengamanan informasi.		
Nama *Framework*	**Cakupan Proses**	**Kejelasan Panduan**	**Penggunaan Secara Umum**
ISO 38500	Terdapat 6 prinsip sebagai *framework* IT *Governance* yang diterapkan untuk tata kelola TI, yaitu *responsibility*, *strategy*, *acquisition*, *performance*, *conformance*, dan *human behaviour*.	Panduan terhadap prinsip-prinsip untuk manajemen organisasi dalam rangka pemanfaatan TI yang tepat guna, efektif dan efisien.	Pengelolaan TI dengan standar tata kelola secara *high-level* yang diterapkan berdasarkan prinsip yang tercantum dalam ISO 38500
TOGAF	Berisi panduan *framework* dan metode pengembangan *Enterprise Architecture* yang meliputi tahapan: a. *Business architecture;* b. *Information architecture;* c. *Application architecture;* d. *Technology architecture;* e. *Transition architecture.*	Panduan terhadap area-area yang harus ada dalam pengembangan *Enterprise Architecture*.	Digunakan untuk mengembangkan *Enterprise Architecture,* dimana terdapat *tools* yang detil untuk mengimplementasikannya.
PMBOK	Berisi panduan kerangka kerja pengelolaan proyek TI dan pengawasan kinerja proyek TI. *Framework* PMBOK	Panduan terhadap area-area kerja yang detil dalam pengelolaan proyek TI.	Sebagai panduan penyusunan kerangka kerja pengelolaan dan pengawasan proyek TI sehingga proyek TI tersebut dapat berjalan sesuai dengan yang diharapkan.

	memberikan referensi lebih detil untuk melengkapi framework COBIT terkait pengelolaan proyek TI.		

IV. TUJUAN DAN SASARAN

IV.1. Tujuan

Tujuan dapat terwujud pelaksanaan tata kelola TI yang baik dengan penerapan pola standarisasi kerangka pengelolaan TI pada setiap Entitas untuk dapat mendukung penerapan GCG secara komprehensif.

IV.2. Sasaran

a. Setiap BUMN diwajibkan memiliki Kebijakan Tata Kelola TI dan *Master Plan* TI untuk penyelarasan pengembangan dan implementasi TI terhadap kebutuhan bisnis masing-masing perusahaan dan menumbuhkan komitmen *top management* Danareksa untuk pengelolaan TI yang terstruktur serta dapat memberikan *Code of Conduct* untuk dapat terselenggaranya TI perusahaan dengan baik;
b. Kepatuhan pada Hak Kekayaan Intelektual (HAKI) akan lisensi *software* (aplikasi) harus dapat dipenuhi oleh masing-masing Entitas. Altematif pemenuhan kepatuhan akan lisensi dapat menggunakan aplikasi *open source*.
c. Target *maturity level* dari Tata Kelola TI Danareksa dalam 5 tahun kedepan adalah minimal *maturity level* 3 sesuai dengan *maturity level* yang ditetapkan,
d. Penyediaan sumber daya TI harus dapat memaksimalkan program sinergi BUMN.

V. *FRAMEWORK* TATA KELOLA TI

Proses tata kelola TI yang perlu dikelola dalam suatu perusahaan dapat dibagi dalam 2 (dua) domain kebijakan, yaitu:

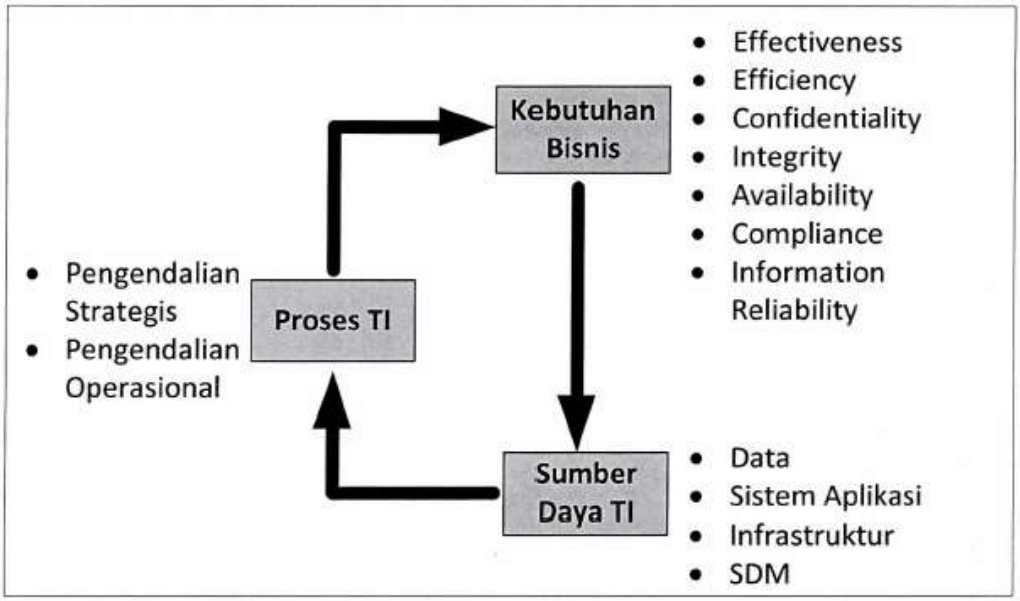
a. Pengendalian Strategis
b. Pengendalian Operasional

Panduan kebijakan TI Danareksa akan mencakup pengendalian TI yang disesuaikan dengan kebutuhan yang berlaku di BUMN.

Kerangka kerja tata kelola TI (*Framework-IT Governance*) yang menjadi standarisasi tata kelola TI pada Danareksa diterapkan pada sumber daya TI yang meliputi aplikasi, perangkat keras, data/informasi, SDM, dan infrastruktur TI (sistem jaringan TI dan sistem komunikasi TI, fasilitas pendukung).

Dengan demikian kebutuhan bisnis perusahaan dapat terpenuhi dari beberapa parameter antara lain: *effectiveness*, *efficiency*, *confidential*, *availability*, *integrity*, *compliance* dan *reliability of information*. Dimana *confidential*, *integrity* dan *availability* terkait dengan sekuriti TI. Sedangkan *effectiveness*, *efficiency* terkait dengan bisnis perusahaan dan *reliability* serta *compliance* terkait dengan performansi manajemen TI.44.

Penerapan kebijakan tata kelola TI dengan basis kerangka kerja tata kelola TI disesuaikan terhadap kondisi lingkungan dan kebutuhan bisnis perusahaan. Untuk itu masing-masing Entitas tidak harus sama penerapan pengendaliannya. Penggunaan pengendalian pada masing-masing Entitas bisa berbeda pada setiap tahunnya disesuaikan terhadap kebutuhan bisnis dan asesmen risiko TI.



Gambar 2. *Framework* Tata Kelola TI

VI. DEFINISI ISTILAH

Asset adalah semua bentuk harta perusahaan termasuk dokumen, surat perjanjian, surat berharga, perlengkapan Direksi dan lain-lain.

Backbone adalah kabel utama yang menghubungkan jaringan komputer antar lantai dengan pusat komunikasi data.

Darurat adalah istilah yang akan disebarluaskan kepada para pegawai tentang situasi/keadaan perusahaan/pegawai yang dilanda musibah bencana alam, gempa bumi, banjir dan kebakaran, serta wabah penyakit.
Data adalah seluruh informasi yang bersifat personal ataupun publik yang menyangkut kegiatan perusahaan yang tersimpan di dalam komputer dan tempat penyimpanan lainnya.

Firewall adalah peralatan yang berfungsi untuk melakukan filter atas paket data yang keluar dari dan masuk ke dalam jaringan komputer Danareksa.

Informasi Danareksa adalah semua data yang berkaitan dengan operasional Danareksa sehari-hari, dalam bentuk apapun seperti *file* elektronik, e-mail, *file transfer*, CD, maupun *hardcopy*-nya.

Jaringan Ekstranet adalah suatu koneksi ke dalam jaringan internal Danareksa oleh suatu jaringan eksternal, yang digunakan untuk sarana pertukaran informasi. Jaringan ekstranet dapat menggunakan *leased line* ataupun VPN sebagai penghubung ke jaringan internal Danareksa.

Jaringan VPN adalah suatu koneksi ke dalam jaringan internal Danareksa oleh suatu jaringan eksternal lainnya, ataupun oleh individual, dengan menggunakan teknologi *tunneling* dan enkripsi seperti IPSec/L2TP atau DES/3DES sebagai pengaman media penghubung, dengan minimal 128 bit encrytor.

Local Area Network **(LAN)** adalah jaringan komputer yang saling berhubungan satu sama lain atau dengan sistem *server* di dalam satu gedung/lokasi Danareksa.

Operational Level Agreement **(OLA)** adalah suatu persetujuan internal antara pihak-pihak internal IT yang mengatur kerjasama mereka dalam mencapai tingkat kualitas layanan yang dikehendaki.

Perangkat Komputer adalah sistem perangkat keseluruhan, berupa CPU, monitor, *keyboard*, *mouse*, beserta alat pendukung lainnya seperti kabel dan adaptor listrik.

Phone Tree adalah diagram berbentuk pohon yang berisi urutan nomor telepon pegawai yang tercatat dalam satu unit kerja yang harus dapat dihubungi secara berantai jika terjadi keadaan darurat /kerusuhan *massal*.

Pos Koordinasi adalah pos koordinasi yang dibentuk dan disiapkan untuk menerima, menyebarluaskan, dan mengelola segala informasi tentang kondisi keamanan dan keadaan

darurat, status siaga, dan informasi banjir di wilayah Jabotabek dan dibuka selama 24 jam setiap hari. Sumber informasi adalah pegawai, aparatur negara, *mass media*, dan lain-lain. Nomor kontak akan ditetapkan melalui Surat Keputusan tersendiri.

Removable Storage adalah semua perangkat penyimpan data yang dapat dipasang atau di-*disconnect* secara mudah dari perangkat komputer. Contohnya, CD-ROM (*drive* dan media CD-nya), *floppy diskette*, *flash disk*, USB *drive*, perangkat pemancar *Bluetooth*, dan lain-lain.
Ruang perangkat teknologi adalah ruangan dimana ditempatkan peralatan teknologi untuk mendukung seluruh kegiatan operasi Danareksa, mitra, gerai dan pihak lain yang mempunyai kerjasama dengan Danareksa. Pada dasarnya ruang perangkat teknologi dibagi menjadi: ruang *server*, ruang telekomunikasi, ruang UPS, ruang IDF, ruang *console* operator. Termasuk dalam definisi ruang perangkat teknologi ini adalah ruangan dimana aksesnya bukan dalam administrasi IT, seperti: ruang *genset*, ruang telekomunikasi/MDF Telkom, dan ruang gas Nitrogen untuk sistem pemadam api.

Sanitasi Data adalah pembersihan data-data sensitif dan bersifat rahasia yang dilakukan sebelum data-data tersebut digunakan oleh pihak lain atau pihak ketiga sehingga keamanan dan kerahasiaan data tetap terjaga.

Service Level Statement **(SLS)** adalah satu pernyataan dari pihak IT sebagai pemberi layanan mengenai tingkat kualitas layanan yang diberikannya, yang sudah sesuai dengan Standar Kualitas Layanan yang ditetapkan dalam kebijakan ini. SLS ini digunakan untuk suatu layanan yang bersifat umum dan digunakan oleh seluruh atau sebagian besar *User* di Danareksa.

Service Level Agreement **(SLA)** adalah satu perjanjian antara pihak IT sebagai pernberi layanan dengan pihak *User* sebagai penerima layanan mengenai tingkat kualitas layanan tersebut, yang sesuai dengan Standar Kualitas Layanan yang ditetapkan dalam kebijakan ini. SLA ini digunakan untuk suatu layanan khusus yang diberikan untuk kelompok *User* tertentu.

Siaga adalah istilah yang akan disebarluaskan kepada para pegawai untuk suatu keadaan kantor/negara dalam situasi tidak terkendali dari massa atau terjadi kerusuhan yang dapat membahayakan kehidupan pegawai atau keluarganya. Status Siaga dibagi menjadi 3 (tiga) yaitu Siaga I, Siaga II, dan Siaga III.

Siaga III adalah kondisi kerusuhan/banjir, gempa (*force majeure*) secara lokal namun tidak mengganggu jalannya perusahaan, pegawai yang tinggal di daerah kerusuhan/*force majeure* dapat diijinkan pulang lebih awal/ tidak masuk bekerja.

Siaga II adalah kondisi kerusuhan/banjir, gempa (*force majeure*) di beberapa tempat yang mempengaruhi ketenangan kerja dan keselamatan pegawai/keluarga. Tingkat bahaya dan kecemasan yang timbul dalam Siaga II ini jauh lebih besar dari Siaga III dimana kantor dapat ditutup dan pegawai diijinkan pulang.

Siaga I adalah kondisi kerusuhan/banjir, gempa (*force majeure*) secara umum yang mempengaruhi kegiatan perusahaan/negara dan sangat membahayakan keselamatan pegawai sehingga kantor harus ditutup sampai keadaan normal kembali. Tingkat bahaya dan kecemasan yang timbul dalam Siaga I ini merupakan yang tertinggi.

Standar Kualitas Layanan (*Service Quality Standard*) adalah suatu standar yang menjadi acuan untuk tingkat kualitas layanan IT, yang akan juga melingkupi suatu sistem pemberian layanan, serta monitoring, pelaporan dan *review* atas parameter-parameter kualitas layanan yang telah ditetapkan atau dijanjikan.

***Wide Area Network* (WAN)** adalah jaringan komputer yang saling berhubungan satu gedung atau lokasi dengan gedung atau lokasi yang berbeda/mempunyai jarak dan harus melalui perangkat *Firewall*.

VII. KEBIJAKAN STRATEGIS TEKNOLOGI INFORMASI (TI)

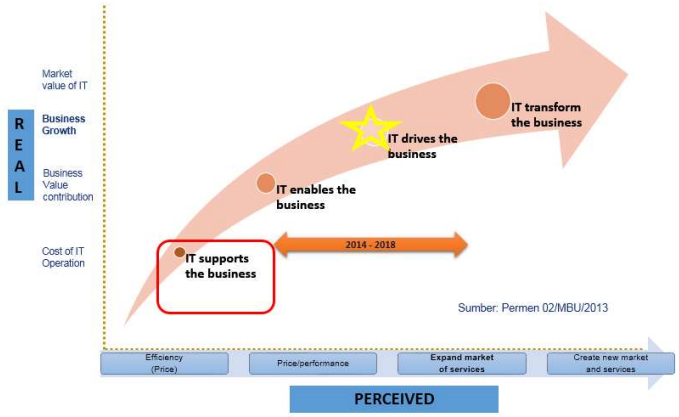
VII.1. Peran TI dalam Perusahaan

Tujuan

Pengembangan TI merupakan salah satu bagian penting dari Perusahaan untuk dapat bersaing dan memberikan dukungan, layanan, kepatuhan, keamanan dan pelaporan, serta menjalankan operasional harian dan pada akhirnya akan memberi manfaat yang sebesar-besarnya bagi Perusahaan.

Ruang Lingkup

Peran TI Perusahaan didefinisikan berdasarkan tujuan strategis diimplementasikannya TI dan IT *Value* di Danareksa. Sebagai gambaran tujuan strategis TI Perusahaan adalah sebagai berikut.



Kebijakan

TI Danareksa pada akhirnya harus menjadi Transformasi Bisnis Perusahaan untuk meningkatkan nilai (*value*) Perusahaan dan untuk mencapai tujuan strategis Perusahaan.

VII.2. Perencanaan TI Perusahaan

Tujuan

Danareksa sebagai suatu perusahaan yang berbasis layanan yang mengandalkan kepada dukungan TI menyadari bahwa TI memiliki peran yang sangat penting dalam pengembangan perusahaan, dalam jangka pendek maupun jangka panjang selain dari kegiatan operasionalnya saat ini. Oleh karena itu, diperlukan adanya *roadmap* dari strategi TI Danareksa sejalan dengan rencana kerja jangka pendek dan jangka panjang perusahaan.

Ruang Lingkup

TI perlu dinyatakan secara jelas untuk menjamin keselarasan bisnis dengan TI, sesuai dengan peran TI dalam perusahaan. Perencanaan TI (*Masterplan* TI) untuk kurun waktu 3 (tiga) sampai dengan 5 (lima) tahun, meliputi:

a. Konteks Bisnis
b. Arsitektur Bisnis
c. IT *Visioning* (visi dan misi TI)
d. Arsitektur Informasi
e. Arsitektur Aplikasi
f. Arsitektur Teknologi
g. Rencana Program TI
h. *Roadmap* Transisi Pengembangan & Implementasi TI

i. IT *Governance* (termasuk didalamnya antara lain Prinsip-prinsip TI, Organisasi TI, Pengelolaan *Governance Enforcement*, Pengelolaan Akuisisi dan Implementasi Solusi TI, Pengelolaan Layanan TI, Pengelolaan Keamanan TI, Pengelolaan Risiko TI, *Transformation Readiness Assessment*)
j. Rencana Sumber Daya TI
k. IT *Valuation*

Kebijakan

a. Danareksa harus memiliki *Master Plan* Teknologi Informasi (MPTI) dalam jangka waktu minimal 3 (tiga) tahun atau sesuai aturan yang ditetapkan oleh perusahaan atau otoritas yang berwenang.
b. MPTI disahkan oleh IT *Committee*, dengan mengacu pada **Lampiran I**.
c. MPTI disusun untuk periode 3 (tiga) sampai dengan 5 (lima) tahun dan diselaraskan dengan Rencana Jangka Panjang Perusahaan (RJPP) dan mendukung strategi dan tujuan perusahaan.
d. MPTI dapat di *review* dan dilakukan pengkinian minimal 1 (satu) kali dalam 1 (satu) tahun apabila diperlukan akibat adanaya perubahan strategi perusahaan dan penyesuaian dengan perkembangan TI terbaru dan mengakomodasi serta mengantisipasi kebutuhan bisnis dan operasional.
e. MPTI diimplementasikan dalam rencana tahunan yang menjadi bagian dari Rencana Kerja dan Anggaran Perusahaan (RKAP).
f. Rencana kerja tahunan harus selaras dan mengacu pada MPTI.
g. MPTI disusun dan ditetapkan oleh Direksi dengan mengacu pada **Lampiran I** Kebijakan ini.
h. Direksi wajib melakukan monitoring dan evaluasi pelaksanaan MPTI secara berkala dan setiap tahun untuk mengetahui keberhasilan pencapaian pelaksanaan, hasil, dan tujuan MPTI.
i. Hasil monitoring dan evaluasi berkala menjadi bagian dari Laporan Manajemen Danareksa yang disampaikan kepada RUPS setiap triwulan dan hasil evaluasi tahunan.
j. Direksi dapat melakukan pengkajian ulang dan melakukan perubahan MPTI yang telah ditetapkan apabila diperlukan untuk mengantisipasi perubahan bisnis dan perkembangan teknologi informasi.

VII.3. Sinergi TI BUMN

a. Setiap BUMN mengutamakan sinergi antar BUMN dalam pemanfaatan dan pengembangan TI.

b. Sinergi antar BUMN sebagaimana dimaksud huruf (a) diutamakan membawa Tingkat Kandungan Dalam Negeri (TKDN) terbesar.
c. Sinergi TI mengacu pada **Lampiran II** Kebijakan ini.
d. Sinergi TI dapat dilakukan pada bidang keuangan, pemasaran, produksi, distribusi, penelitian, pengadaan, SDM dan TI.
e. Pelaksanaan sinergi TI dilakukan berdasarkan azas manfaat yang berlandaskan pada prinsip-prinsip GCG.

VII.4. Kerangka Kerja Proses dan Organisasi TI

Tujuan

Kebijakan ini bertujuan agar proses utama TI Perusahaan dapat dijalankan dan selaras dengan peran TI Perusahaan, serta tersedianya organisasi pendukung proses tersebut.

Ruang Lingkup

Kerangka kerja proses TI harus didefinisikan yang meliputi struktur proses, *ownership*, *performance measurement* & *compliance*.
Organisasi fungsional TI disusun berdasarkan kaidah pemisahan tugas sesuai fungsi atau *Segregation of Duty* (SoD) yang meliputi fungsi-fungsi:
a. Pengelolaan Strategi dan Perencanaan Strategis TI.
b. Pengelolaan Layanan TI
c. Pengembangan TI
d. Pengelolaan Operasi TI
e. *Monitoring* & *Control* TI.

IT *Steering Committee* (Komite Pengarah TI) dibentuk untuk penentuan prioritas program, persetujuan anggaran, dan keputusan implementasi program TI perusahaan sesuai dengan kebutuhan bisnis Perusahaan.

Kebijakan

a. Susunan IT *Steering Committee* terdiri dari Direksi Induk Perusahaan dan Direktur Anak Perusahaan dan diketuai oleh Dirut Induk Perusahaan serta dibantu oleh Sekretaris *Committee*.
b. IT *Steering Committee* di ketuai oleh Direktur Utama dan beranggotakan Direksi Anak Perusahaan, Kepala Divisi IT Induk dan Anak Perusahaan.
c. Divisi *Corporate Secretary* Induk Perusahaan bertindak sebagai sekertaris IT *Committee*.

d. IT *Steering Committee* bekerja sesuai dengan *job descriptions* yang telah di tetapkan oleh Direksi.
e. Keanggotaan IT *Steering Committee* ditetapkan dalam Surat Keputusan (SK) tersendiri yang diterbitkan oleh Komite Pengelolaan Risiko Induk Perusahaan.

VII.5. Pengelolaan Investasi

Tujuan

Memastikan bahwa setiap investasi TI selaras dengan strategi bisnis perusahaan dan *Master Plan* Teknologi Informasi (MPTI) yang telah dibuat.

Ruang Lingkup

Pengelolaan investasi TI Perusahaan merupakan bagian dari proses pengembangan, operasi, dan pemeliharaan sistem informasi yang harus dilaksanakan dalam kerangka MPTI. Strategi pendanaan investasi atau pembiayaan TI dapat pula diatur pada kebijakan ini. Salah satu pendekatan anggaran penentuan pembiayaan (*spending*) TI adalah prosentase dari *revenue* perusahaan (setiap industri rata-rata prosentasenya berbeda-beda).

Kebijakan

a. *Roadmap* atau rencana investasi yang dituangkan dalam *Master Plan* dan pengelolaan Rencana Kegiatan dan Anggaran Perusahaan (RKAP) bidang TI.
b. Setiap tahun Divisi IT menyiapkan Rencana Kerja dan Anggaran Perusahaan dalam bidang pengembangan, operasional dan pemeliharaan TI Danareksa Grup bersama Divisi Business Development masing-masing Entitas.
c. Sebagai *Cost Center*, Divisi IT dalam melakukan penggunaan anggaran TI harus tunduk dengan kebijakan penggunaan anggaran yang telah ditetapkan oleh Danareksa.

VII.6. Pengelolaan Sumber Daya TI

VII.6.1. Pengelolaan Sumber Daya Manusia

Tujuan

Kebijakan ini bertujuan agar seluruh proses pengelolaan sumber daya TI dapat dikelola sesuai dengan aturan-aturan yang dipersyaratkan sehingga dapat menghasilkan produk TI yang dapat dipercaya, efektif dan efisien.

Ruang Lingkup

Kebijakan pengelolaan sumber daya TI meliputi kebijakan-kebijakan yang mengatur:

a. Sumber Daya Manusia

Kebijakan pengelolaan sumber daya manusia TI dapat merupakan bagian dari kebijakan pengelolaan SDM perusahaan secara umum, ataupun dibuat kebijakan secara khusus, yang pada umumnya meliputi:

i. Rekrutasi dan pengelolaan kompetensi;
ii. Pendefinisian peran dan tugas suatu posisi termasuk monitoring dan supervisi posisi yang didefinisikan;
iii. Pelatihan SDM;
iv. Pengelolaan *knowledge* agar dapat meminimalkan ketergantungan terhadap individu tertentu;
v. *Prosedure clearance* (apabila diperlukan);
vi. Perubahan dan pemberhentian tugas; dan
vii. Penilaian dan evaluasi performansi karyawan.

b. Data/Informasi

Kebijakan pengelolaan sumber daya data atau informasi meliputi proses proses akuisisi data yang dapat menjamin kelengkapan (*completeness*), akurasi (*accuracy*), validitas (*validity*), dan autorisasi (*authorization*) data yang biasanya didefinisikan dalam suatu *manual application control* dari suatu bisnis proses dengan mempertimbangkan pemisahan tugas (*segregation of duty*) dari pihak-pihak penyedia.

Proses lain yang diatur dalam kebijakan pengelolaan data adalah bagaimana memproteksi dan memelihara data agar tingkat kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan data (*availability*) tetap terjaga.

c. *Software*/Aplikasi

Kebijakan pengelolaan sumber daya *software* (aplikasi) meliputi kebijakan proses pengelolan akusisi, pengelolaan operasi dan pemeliharaan aplikasi/*software* yang telah beroperasi. Pengelolaan akuisisi aplikasi dapat berupa proses pengembangan secara mandiri (*self/inhouse developed*), *Commercial Off-The-Shelf* (COTS)/*Package* yang berupa pembelian aplikasi yang telah siap digunakan, *Joint Development* dengan pihak ketiga dan sewa pakai aplikasi atau *sharing income/revenue* dengan pihak bisnis terkait. Umumnya proses ini dituangkan dalam suatu standar yang umum disebut *Software Development Life Cycle* (SDLC), sehingga dalam kebijakannya dapat dinyatakan secara garis besarnya saja yang pada intinya adalah

proses akusisi software/aplikasi harus selaras dengan kebutuhan bisnis dengan memperhatikan persyaratan *security*, *availability*, *maintainability* dan *auditability*.

d. Infrastruktur
Kebijakan pengelolaan sumber daya teknologi infrastruktur meliputi kebijakan proses pengelolaan akusisi infrastruktur dengan mempertimbangkan persyaratan *security* & *availabiity*, operasi dan pemeliharaan infrastruktur serta penyediaan *environment* untuk pengembangan atau pengujian aplikasi.

e. Tata kelola pengadaan sumber daya TI
Kebijakan tata kelola pengadaan sumber daya TI dapat merupakan kebijakan pengadaan secara umum ataupun dibuat kebijakan khusus TI dengan mempertimbangkan strategi penyampaian layanan TI, standarisasi dan integrasi infrastruktur TI dan mengurangi risiko pengadaan sumber daya TI. Kebijakan ini meliputi proses pengendalian pengadaan, cara pemilihan pemasok (*supplier*), dan manajemen kontrak untuk meningkatkan efisiensi biaya TI dan kontribusi TI terhadap bisnis.

Kebijakan

a. Kebijakan pengelolaan sumber daya TI ini pada umumnya menghasilkan standar dan prosedur yang mengatur tata cara penyediaan dan pengelolaan sumber daya TI, yang antara lain berupa: standar pengembangan aplkasi (*Software Development Life Cycle*/SDLC), standar teknologi infrastruktur TI, prosedur akusisi aplikasi, data dan infrastruktur, dan prosedur terkait lainnya.
b. Pengelolaan sumber daya manusia di Divisi IT mengikuti kebijakan, peraturan dan ketentuan yang berlaku di PT. Danareksa (Persero) dan anak perusahaan.
c. Pengelolaan sumber daya manusia di Divisi IT mengikuti Perjanjian Kerja Bersama antara PT. Danareksa (Persero) dan Anak Perusahaan dengan serikat pekerja Danareksa (Danareksa Club).

VII.6.2. Pengelolaan *Software* dan Aplikasi

Tujuan

Kebijakan ini mencakup penggunaan *software* dan standar yang telah ditetapkan oleh Danareksa dan juga *software* lainnya yang digunakan oleh pegawai Danareksa sesuai dengan kebutuhan. Penggunaan yang diatur dalam kebijakan ini adalah penggunaan yang sesuai dengan strategi Danareksa, dengan *license agreement* masing-masing *software* yang digunakan, dan juga sesuai dengan peraturan perundangan yang berlaku.

Ruang Lingkup

Kebijakan ini mencakup penggunaan seluruh *software* yang ter-*install* dalam komputer Danareksa, termasuk OS (*server* dan *workstation*), *Office application*, antivirus (*server* dan *workstation*), *software platform Database Management System* (DBMS/RDBMS), *three-tier web application* dan lain-lain.

Kebijakan

a. Dalam hal akuisisi aplikasi TI akan dilihat dari kebutuhan dan kompleksitas dari aplikasi yang akan di akuisisi, dengan cara:
   i. Melakukan pengembangan/*development* secara internal.
   ii. Membeli aplikasi yang sudah jadi untuk diimplementasikan di Danareksa dan disesuaikan dengan kebutuhan Danareksa.
   iii. Melakukan *join development* dengan Perusahaan Penyedia Jasa layanan pengembangan aplikasi.
b. Seluruh proses tersebut di atas harus mengikuti kebijakan pengadaan yang berlaku di Danareksa.
c. TI membuat suatu standar *software* yang akan direkomendasikan untuk di-*install* pada setiap komputer pegawai dan digunakan dalam tugas operasionalnya sehari-hari. *Software* standar tersebut telah dianggap dapat memenuhi kebutuhan operasional masing-masing pegawai Danareksa sehari-hari dengan memperhatikan uraian tugas dan tanggung jawabnya. Penggunaan *software* standar ini akan diatur Danareksa dari segi lisensi-nya.
d. Pegawai tidak diperbolehkan untuk melakukan *install software* lainnya tanpa sepengetahuan dan persetujuan IT. Jika hal ini terjadi, maka segala konsekuensi yang diakibatkan oleh *software* tersebut, misalnya komputer *crash*, terserang virus, atau terkait dengan masalah hukum yang berlaku sepenuhnya menjadi tanggung jawab pegawai yang bersangkutan dan merupakan pelanggaran yang dapat dikenakan sanksi sesuai peraturan kepegawaian yang berlaku.
e. Penggunaan *software* yang tidak mempunyai lisensi akan menjadi tanggung jawab masing-masing pengguna dimana Danareksa dibebaskan dari segala tuntutan dan tanggung jawab mengenai penggunaan *software* ilegal tersebut.
f. IT Danareksa akan melakukan audit internal secara berkala terhadap penggunaan *software*-nya.
g. Pegawai dilarang memiliki, menggunakan, menyebarkan *software* ataupun barang-barang yang dilindungi oleh hak cipta lainnya seperti *game*, MP3, CD musik, ataupun media lainnya di dalam lingkungan Danareksa.

h. Segala pelanggaran terhadap kebijakan dan peraturan ini dapat dikenakan sanksi seperti yang diatur dalam Kebijakan Penanganan Insiden dan Sanksi.

VII.6.3. Pengelolaan Data atau Informasi

Tata Kelola Akses Data dan Informasi
Sharing data antar Entitas dalam grup antara lain untuk kepentingan kerjasama antar Entitas, maupun pemenuhan regulasi, dilakukan dengan memperhatikan dan sesuai dengan mekanisme tata kelola dan regulasi yang berlaku. Ketentuan tersebut selanjutnya akan diatur dalam kebijakan yang mengatur hubungan antar Entitas dalam grup.

A. Pemilik Data
Tujuan
Untuk memastikan kepemilikan data dalam rangka menentukan hak akses atas data yang penyimpanannya dikelola oleh Divisi IT.

Ruang Lingkup
Kebijakan ini mencakup semua informasi dan data milik Danareksa yang diwakili oleh Divisi terkait pemilik dan pengelola informasi dan data tersebut.

Kebijakan
a. Pemilik data adalah divisi yang mempunyai hak untuk melakukan pembuatan, perubahan/modifikasi dan penghapusan data/informasi.
b. Setiap pemberian akses terhadap data harus di lakukan dengan seizin pemilik data yaitu divisi sebagai pengelola informasi/data tersebut.
c. Setiap penggunaan data untuk keperluan pengujian aplikasi oleh pihak ketiga, harus diketahui dan seizin Direksi dari Entitas pemilik data.
d. Setiap penggunaan data untuk keperluan pegujian aplikasi baik oleh internal Danareksa atau pihak ketiga harus dilakukan sanitasi data.

B. Penyimpanan Data
Tujuan
Untuk memastikan bahwa akses terhadap informasi Danareksa hanya diberikan kepada dan dilakukan oleh mereka yang berhak dan telah mendapatkan akses tersebut sesuai dengan prosedur yang berlaku. Hal ini juga berlaku untuk meningkatkan keamanan akses terhadap informasi yang disediakan oleh Danareksa dan melindungi kerahasiaan

data sesuai kepentingan Danareksa maupun pemenuhan ketentuan peraturan yang berlaku.

Ruang Lingkup

Kebijakan ini mencakup semua informasi dan data milik Danareksa, terutama yang terbatas aksesnya, dan termasuk media untuk akses seperti *file server* dan jalur telekomunikasi yang digunakan.

Kebijakan

a. *Backup* data milik Danareksa tidak boleh disimpan dalam satu lokasi yang sama dengan data *production*.
b. Salah satu *copy* data harus disimpan dilokasi diluar kantor Danareksa dengan tidak menutup kemungkinan menggunakan jasa pihak ketiga yang menyediakan jasa penyimpanan media *backup*.
c. Tempat penyimpanan media *backup* harus dapat memenuhi standar penyimpanan agar media *backup* dapat bertahan lama, minimal sesuai aturan retensi data yang ditetapkan oleh perusahaan dan peraturan yang berlaku.
d. Tempat penyimpanan media *backup* harus memiliki keamanan yang memadai dan akses yang hanya dapat dilakukan oleh staf Danareksa dan petugas media penyimpanan media *backup* yang mempunyai kewenangan.
e. Untuk setiap data yang tersimpan, harus dilakukan kebijakan retensi masing-masing, yang akan digunakan sebagai pedoman IT untuk memastikan bahwa data harus dapat diakses kembali dalam keadan utuh. Hal ini akan disesuaikan dengan ketentuan Danareksa maupun peraturan perundangan yang berlaku.
f. Berdasarkan klasifikasi atas informasi yang diberikan, maka harus dilakukan pembedaan sistem akses dan *backup* yang dipilih, yang nantinya akan membuat data yang sangat dibutuhkan oleh operasional Danareksa mendapat perhatian semestinya dan dapat diakses secara kontinyu.
g. Suatu sistem *backup* harus dipilih untuk semua informasi yang disimpan di *file server*, dimana pelaksanaannnya harus sesuai dengan huruf (a) di atas.
h. Penyimpanan media *backup* harus mengikuti peraturan yang berlaku, untuk peletakan media *backup* di lokasi *offsite*.
i. Untuk media *back up* dengan peralatan yang lama atau tidak di-*support* oleh vendor maka Divisi IT harus menjaga atau mempunyai peralatan *restrore* tersebut atau Divisi IT harus melakukan *convert* data *back up* tersebut ke peralatan baru.

j. Apabila data yang harus di-*restore* berada pada lokasi *offsite*, maka kecepatan pengambilan kembali dan proses *restore* yang diperlukan harus dapat diterima oleh para pemilik data sesuai atau memenuhi *service level* yang dikerjakan.

C. *Backup* dan *Restore* Data

Tujuan

Untuk memastikan bahwa penyimpanan data sesuai dengan tujuan untuk mendukung operasional Danareksa.

Ruang Lingkup

Kebijakan ini mencakup seluruh media penyimpan data dengan proses penyimpanan, *restore*, dan penghancuran masing-masing media. Tujuannya adalah supaya informasi perusahaan dapat diakses oleh mereka yang berhak saat diperlukan.

Kebijakan

a. Untuk setiap data tersimpan, harus dilakukan kebijakan retensi masing-masing, yang akan digunakan sebagai pedoman TI untuk memastikan tingkat reliabilitas data termaksud. Hal ini akan disesuaikan dengan ketentuan Danareksa maupun peraturan perundangan yang berlaku.
b. Berdasarkan klasifikasi atas informasi yang diberikan, maka harus dilakukan pembedaan sistem akses dan *backup* yang dipilih, yang nantinya akan membuat data yang sangat dibutuhkan oleh operasional Danareksa mendapat perhatian semestinya dan dapat diakses secara kontinyu.
c. Suatu sistem *backup* harus dipilih untuk semua informasi yang disimpan di *file server*, dimana pelaksanaannya harus sesuai dengan huruf (a) di atas.
d. Penyimpanan media *backup* harus mengikuti peraturan yang berlaku, untuk peletakan media *backup* di lokasi *offsite*.
e. Tempat penyimpanan media *backup* harus disesuaikan dengan persyaratan yang ada, untuk meminimalkan risiko kegagalan *restore* karena media yang rusak. Persyaratan yang sama harus dipenuhi oleh lokasi *offsite* yang dipilih.
f. Semua proses *backup* harus didokumentasikan dengan lengkap dan *reliable*, untuk mempermudah proses *restore* data tersebut dimana diperlukan. Semakin tinggi kebutuhan akan data maka semakin cepat proses *restore* dilakukan. Kemungkinan media *backup* tidak terlacak harus ditekan sekecil mungkin.
g. Dilakukan *test* secara periodik atas media *backup* yang ada, untuk memastikan bahwa data pada media tersebut dapat di-*restore* dengan baik. Setiap *test* yang dilakukan akan didokumentasikan secara formal.

D. Pengelolaan Konfigurasi Infrastuktur

Tujuan

Untuk memastikan bahwa perubahan konfigurasi infrastuktur yang digunakan oleh Perusahaan dapat didokumentasikan dengan baik dan aman.

Ruang Lingkup

Kebijakan ini mencakup perubahan, perbaikan dan monitoring konfigurasi infrastruktur yang digunakan oleh Perusahaan tidak terbatas untuk operasional, *User Acceptance Test* (UAT) dan *development* baik di kantor pusat, kantor cabang maupun di lokasi DRC yang telah ditetapkan.

Kebijakan

a. Setiap perubahan konfirgurasi harus mengkuti kebijakan prosedur yang berlaku di Perusahaan.
b. Setiap perubahan konfigurasi harus didokumentasikan dengan baik.
c. Setiap perubahan atau perbaikan konfigurasi infrastruktur harus di lakukan uji coba pada lingkungan UAT atau *Development* terlebih dahulu sebelum di implementasikan pada lingkungan produksi berdasarkan persetujuan yang mengacu kepada hasil UAT.
d. Pengecualian pada poin tersebut di atas dapat dilakukan jika dipandang perlu untuk dilakukan perubahan konfigurasi infrastruktur langsung pada lingkungan produksi dengan persetujuan dari Kepala Divisi IT atau staf yang ditunjuk sebagai penggantinya.

E. Pengelolaan Kinerja dan Kapasitas Sistem TI

Tujuan

Memastikan seluruh sumber daya TI baik *hardware* dan *software* untuk mendukung kegiatan bisnis dan operasional dapat berjalan dengan normal tanpa terhenti karena adanya keterbatasan sumberdaya *hardware* dan *software* yang digunakan dengan melakukan perencaan kapasitas sumberdaya dengan baik.

Ruang Lingkup

Kebijakan ini mencakup atas perencaaan dan pengelolaan kapasitas Sistem TI dalam hal ini *hardware* dan *software* yang digunakan untuk kegiatan bisnis dan operasional perusahaan baik di kantor pusat maupun di lokasi DRC yang telah di tetapkan.

Kebijakan

a. Setiap awal tahun atau pada saat perencanaan anggaran Divisi IT harus melakukan evaluasi dan perencanaan kapasitas *hardware* dan *software* yang digunakan untuk operasional di kantor pusat dan lokasi DRC dengan mengacu kepada rencana pengembangan yang akan dilakukan.
b. Evaluasi atas kapasitas *hardware* dan *software* harus dilakukan minimal 1 (satu) tahun 1 (satu) kali.
c. Berdasarkan hasil evaluasi ini dilakukan perencanaan dan penyesuaian/ pembaharuan kapasitas sistem TI untuk memenuhi kebutuhan bisnis dan operasional perusahaan.
d. Secara regular Divisi IT harus melakukan monitoring terhadap kinerja dan kapasitas sistem yang sedang berjalan untuk memastikan kinerja sistem TI berjalan dengan baik sesuai kebutuhan operasional perusahaan.
e. Dalam rangka perencanaan dan implementasi sistem, Divisi IT harus memastikan bahwa kinerja dan kapasitas sistem telah sesuai dengan kebutuhan perusahaan yang juga memperhitungkan perkiraan pertumbuhan bisnis dimasa yang akan datang.

VII.7. Pengelolaan Proyek TI

Tujuan

Memastikan seluruh proyek yang dikelola oleh Divisi IT dapat berjalan, teradministrasi dan termonitor dengan baik sesuai spesifikasi yang direncanakan dan tepat waktu.

Ruang Lingkup

Kebijakan ini mencakup seluruh proyek yang dikelola oleh Divisi IT dan proyek yang dikelola secara bersamaan dengan Divisi lain diluar Divisi IT.

Kebijakan

a. Divisi IT harus memiliki unit atau staf yang berfungsi sebagai *Project Management Office* untuk melakukan pengelolaan, administrasi, monitoring dan pelaporan seluruh proyek yang dikelola oleh Divisi IT ataupun proyek yang dikelola bersama Divisi lain.
b. *Project Management Office* dapat merekomendasikan saran-saran dan tindakan yang harus dilakukan oleh *Project Manager* dalam kaitan penyelesaian proyek.
c. *Project Management Office* turut memantau kesesuaian waktu dan *progress* proyek, seperti pemenuhan *service level*.
d. *Project Management Office* mengadministrasikan dan mendokumentasikan proyek secara memadai.

VII.8. Pengelolaan Risiko TI

Tujuan

Kebijakan ini bertujuan agar risiko-risiko akibat diimplementasikannya TI atau tidak beroperasinya TI sebagai pendukung bisnis dapat diidentifikasikan dan dilakukan mitigasi yang tepat.

Ruang Lingkup

Kebijakan pengelolaan risiko TI meliputi pengaturan proses identifikasi risiko TI dalam suatu asesmen/penilaian risiko (*risk assessment*), dampak potensialnya terhadap bisnis dan tujuan perusahaan serta rencana mitigasinya yang merupakan tanggapan dari hasil identifikasi risiko.

Kebijakan

Kebijakan ini dapat menghasilkan standar atau prosedur kerangka kerja pengelolaan risiko TI yang terintegrasi dengan kerangka kerja pengelolaan risiko perusahaan.

VIII. PENGELOLAAN LAYANAN TEKNOLOGI INFORMASI

VIII.1. Pengelolaan Layanan TI

Tujuan

Kebijakan pengelolaan layanan TI adalah kebijakan yang mengatur tata kelola layanan TI yang bertujuan agar proses layanan TI dapat teridentifikasi dan di definisikan dengan baik untuk mencapai kinerja yang diharapkan dengan kelangsungan layanan TI perusahaan.

Ruang Lingkup

Seluruh layanan yang diberikan secara rutin dan operasional oleh pihak TI kepada *User* sesuai dengan pemenuhan *service level* dan perjanjian kerjasama antar perusahaan, baik dilakukan sendiri atau dengan melibatkan pihak ketiga.

Kebijakan pengelolaan layanan TI meliputi antara lain proses-proses:

a. Tahapan *Service Strategy*
   i. Pengelolaan *Service Portfolio* (*Service Portfolio Management*)
      Definition note: Service Portfolio Management is a dynamic method for governing investments in service management across the enterprise and managing them for value. (*Reference source*: ITIL v3-*Service Strategy Book*).
      Proses pengelolaan portofolio layanan yang bertujuan memberikan arahan strategis dan pengelolaan investasi pada pengelolaan layanan TI, sehingga portofolio layanan yang optimal tetap dapat dipelihara.

ii. Pengelolaan Keuangan Layanan TI (*Financial Management*)

Definition note: The function and processes responsible for managing an IT Service Provider's Budgeting, Accounting and Charging Requirements. (*Reference source* : ITIL v3-*Service Strategy Book*)

Proses pengelolaan keuangan layanan TI yang meliputi pengelolaan anggaran dan penagihan biaya dari penyedia layanan TI.

Kontrak yang dilakukan *User* dengan penyedia layanan TI, harus mencantumkan hal yang terkait dengan harga, seperti perubahan terhadap lingkup layanan, kesepakatan atas parameter yang digunakan dalam menentukan harga, dan prosedur dalam menyelesaikan permasalahan atas ketidaksepakatan atas harga yang ditentukan.

iii. Pengelolaan Permintaan Layanan TI (*Demand Management*)

Definition note: Activities that understand and influence Customer demand for services and the provision of Capacity to meet these demands. (*Reference source*: ITIL v3-*Service Strategy Book*).

User dapat melakukan persetujuan terhadap personil penyedia layanan TI yang ditunjuk dan mempunyai wewenang mendefinisikan kriteria yang digunakan dalam memilih personil tersebut.

b. Tahapan *Service Design*

i. Pengelolaan Katalog Layanan TI (*Service Catalogue Management*)

Definition note: Service Catalogue Management is to provide a single source of consistent Information on all of the agreed services, and ensure that is widely available to those who are approved to access it. (*Reference source*: ITIL v3-*Service Design Book*)

ii. Pengelolaan Tingkat layanan TI (*Service Level Management*)

Proses pengelolaan tingkat layanan TI adalah proses yang mengelola perjanjian tingkat layanan TI dengan pengguna, serta pelaporan hasil layanan TI selama dijaminkan. Pengelolaan tingkat layanan dapat dikaitkan dengan pola *charge back* (jika diterapkan) untuk menyelaraskan kualitas layanan yang diberikan dengan upaya layanan TI yang dilakukan pengelola TI.

iii. Pengelolaan Kapasitas (*Capacity Management*)

Proses pengelolaan kapasitas infrastruktur layanan TI adalah proses yang mengelola penggunaan sumber daya infrastruktur TI dan proses pemenuhan

kebutuhan kapasitas infrastruktur untuk layanan TI yang dijaminkan agar tetap memiliki kinerja dan tingkat ketersediaan yang baik.

iv. Pengelolaan Ketersediaan Layanan TI (*Availability Management*)
Proses pengelolaan ketersediaan layanan TI adalah proses yang mengelola ketersediaan layanan TI baik *software*/aplikasi, infrastruktur dan jaringan agar tetap dapat beroperasi sesuai dengan tingkat layanan yang dijaminkan.

v. Pengelolaan Kesinambungan Layanan TI (*Service Continuity Management*)
Proses pengelolaan kesinambungan layanan TI adalah proses yang mengelola kesinambungan layanan TI agar tetap dapat beroperasi sesuai dengan tingkat layanan yang dijaminkan. Salah satu upayanya antara lain dengan adanya *Disaster Recovery Plan* (DRP) untuk layanan kritikal.

c. Tahapan *Service Transition*

i. Pengelolaan Perubahan (*Change Management*)
Proses pengelolaan perubahan seluruh aspek layanan TI yang berupa identifikasi permintaan perubahan, identifikasi dampak akibat perubahan layanan TI, pelaksanaan perubahan layanan TI, dan pelaporan perubahan layanan TI.

ii. Pengelolaan Konfigurasi (*Service Asset and Configuration Management*)
Proses pengelolaan konfigurasi adalah proses yang mengelola pencatatan konfigurasi sistem layanan TI baik berupa aplikasi maupun infrastruktur serta tata cara perubahan konfigurasi yang diperlukan.

iii. *Release and Deployment Management*
Proses pengelolaan *release* atau versi aplikasi adalah proses yang berupa identifikasi pencatatan versi aplikasi yang beroperasi, penyimpanan *source* aplikasi yang dioperasikan, dan proses validasi bahwa versi aplikasi yang dioperasikan sama dengan *source* versi aplikasi yang disetujui untuk dioperasikan.

iv. *Service Validation and Testing*
Definition note: The process responsible for Validation and testing of a new or changed IT service. Service Validation and Testing ensures that IT Service matches its design specification and will meet the needs of the business. (*Reference source*: ITIL v3-*Service Transition Book*)

v. *Knowledge Management*
Definition note: The process responsible for gathering, analysing, storing and sharing knowledge and information within an Organization. The primary purpose of Knowledge Management is to improve Efficency by reducing the need to rediscover knowledge. (*Reference source*: ITIL v3- *Service Transition Book*)

d. Tahapan *Service Operation*

i. *Service Desk*
Pengelolaan fungsi layanan untuk penerimaan laporan insiden, gangguan, keluhan, dan permintaan layanan TI yang pada umumnya berupa *call center* atau *helpdesk*.

ii. *Event Management*
Definition note: The process that monitors all events that occur through the IT infrastructure to allow for normal operation and also to detect and escalate exception conditions. (*Reference source*: ITIL v3-*Service Operation Book*)

iii. Pengelolaan Insiden Layanan TI *(Incident Management)*
Proses pengelolaan insiden layanan TI yang berupa penerimaan laporan insiden, penanganan insiden, eskalasi dan pelaporan insiden layanan TI.

iv. Pengelolaan Permasalahan Layanan TI *(Problem Management)*
Proses pengelolaan permasalahan layanan TI yang berupa identifikasi masalah dari laporan insiden, penyelesaian masalah, eskalasi permasalahan dan pelaporan permasalahan layanan TI.

v. Pengelolaan Permintaan Layanan TI *(Request Fulfilment)*
Definition note: The process for dealing with service requests-many of them actually smaller, lower-risk, changes-initially via Service Desk, but using a separate process similar to that of Incident Management but with separate Request fulfilment records/tables-where necessary linked to the Incident/Problem record(s) that initiated the need for the request. (*Reference source*: ITIL v3-*Service Operation Book*).

vi. Pengelolaan Akses *(Access Management)*

Definition note: The process for granting authorized users the right to use a service, while restricting access to non-authorized users. It is based on being able accurately to identify authorized users and then manage their ability to access services as required during different stages of their Human Resources (HR) or contractual lifecycle. (*Reference source*: ITIL v3-*Service Operation Book*).

e. Tahapan *Continual Service Improvement*
   i. *Continual Service Improvement (7-Step) process*
   Continual Service Improvement uses the 7-Step Improvement process as following:
      1. *Define what you should measure*;
      2. *Define what you can measured*;
      3. *Gathering the data*;
      4. *Processing the data*;
      5. *Analysing the data*;
      6. *Presenting and using the information*; *and*
      7. *Implementing corrective action*.

      (*Reference source*: ITIL v3-*Continual Service Improvement Book*)

   ii. *Service Measurement and Reporting*
   To coordinate the design of metrics, data collection and reporting activities from the other processes and functions.

Tanggung Jawab

a. Divisi IT bertanggung jawab untuk mengelola layanan yang disediakannya sesuai kewenangannya yang tercakup dalam kebijakan ini.
b. Setiap pegawai Danareksa diharapkan mengetahui proses pengelolaan layanan TI sehingga kinerja layanan dapat dimanfaatkan dengan optimal.

Kebijakan

a. Divisi IT menyediakan portofolio layanan sesuai arah strategis Danareksa yang sekurangnya mencakup layanan terhadap nasabah, internal, afiliasi Danareksa maupun regulator.
b. Layanan TI dikelola oleh unit atau staf IT yang diberi wewenang sekurangnya untuk melakukan pemeriksaan, memelihara, perubahan, perbaikan dan pelaporan terhadap atasan sesuai struktur organisasi yang diatur dalam prosedur terkait.

c. Seluruh pengadaan perangkat atau jasa sistem TI harus mengikuti kebijakan dan prosedur pengadaan barang dan jasa yang diberlakukan oleh PT. Danareksa (Persero).
d. Kegiatan pemeliharaan layanan TI dilakukan secara berkala atau dalam kondisi tertentu dapat dilakukan sesuai kebutuhan bisnis Danareksa.
e. Divisi IT mengelola ketersediaan layanan TI baik dalam bentuk *software* dan *hardware* serta memastikan kapasitas sumber daya infrastruktur IT dan *Standard Operating Manual* (SOM) memenuhi mutu layanan dan tingkat layanan yang dijaminkan sesuai standar layanan IT Danareksa.
f. Kejadian insiden, permasalahan dan perubahan terhadap layanan TI harus teridentifikasi penyelesaiannya dan didokumentasikan sesuai prosedur layanan TI.
g. Kontrak antara penyedia layanan TI dan *User*, harus sesuai dengan peraturan perundang-undangan dan hukum yang berlaku di Indonesia. Termasuk dari tata Bahasa harus dapat mendefinisikan prosedur dan proses dalam identifikasi, diskusi, eskalasi, resolusi sampai dengan level manajemen atas suatu permasalahan.
h. Proses pengelolaan perubahan sekurangnya mencakup identifikasi permintaan, persetujuan, klasifikasi, prioritas dan dampak perubahan. Kontrak harus dapat melindungi *User* dengan memiliki wewenang untuk merubah kontrak, hubungan kerjasama dan batasan dari kontrak, supaya dapat sesuai dan beradaptasi dengan perubahan di lingkungan bisnis *User* terutama yang terkait dengan regulasi.
i. Bila terjadi perubahan yang signifikan harus dilakukan review dan proses validasi atau *User Acceptance Test* (UAT) untuk memastikan layanan TI sesuai dengan spesifikasi desain dan memenuhi kebutuhan bisnis dan operasional.
j. Pengelola layanan TI mendokumentasikan *configuration baseline* atas sistem layanan TI baik berupa aplikasi maupun infrastruktur serta cara perubahan konfigurasi yang diperlukan.
k. Pengelola layanan harus melakukan langkah pengamanan yang tepat untuk dapat melindungi sistem layanan dari penggunaan atau perubahan tanpa izin atas sistem TI.
l. Divisi IT menjaga kerahasiaan data perusahaan melakukan perlindungan data terhadap kebocoran informasi ke pihak luar melalui *Non Disclosure Agreement* (NDA) dengan penyedia layanan TI serta menggunakan data *dummy* pada saat melakukan pengembangan atau pengujian sistem TI. Apabila diperlukan, penyedia layanan IT melakukan pelatihan *Employee Awareness*, serta mencantumkan Kewajiban Penyedia Layanan IT dan pasal ganti rugi jika terdapat pelanggaran yang dilakukan dalam Kontrak.

m. Kesinambungan sistem TI harus dikelola agar layanan tetap beroperasi sesuai standar mutu yang ditetapkan. Layanan yang kritikal sekurangnya harus memiliki *backup* sistem, kontinjensi atau *Business Continuity Plan* (BCP).
n. Layanan TI yang didukung oleh penyedia layanan TI harus memiliki perjanjian tertulis dan melakukan evaluasi kinerja vendor untuk memastikan penyedia jasa memelihara layanan dan keamanan sesuai dengan perjanjian kerjasama. Dalam hal penyedia layanan menggunakan jasa pihak ketiga (contoh: subkontrak) dalam menyediakan layanan, *User* harus dilibatkan dalam menentukan kualitas layanan yang akan diberikan termasuk diantaranya tindakan-tindakan dalam meminimalkan resiko yang mungkin timbul.
o. Mengkomunikasikan komitmen pelayanan dalam laporan hasil layanan dan melakukan evaluasi secara perkala terhadap kinerja sistem layanan TI.
p. Dalam hal Penyedia layanan menggunakan sumberdaya dari User, maka aturan, prosedur dan kepemilikan atas sumberdaya tersebut harus didefinisikan dan diberlakukan.
q. Jika dalam suatu aktivitas penggunaan Jasa layanan menghasilkan suatu produk atau nilai tambah terhadap sumberdaya yang ada, hak kepemilikan serta prosedur dan atas hal tersebut harus didefinisikan dalam kontrak/perjanjian
r. Kontrak harus memastikan bahwa *User* mendapatkan informasi tentang kemungkinan peristiwa yang terkait kemampuan penyedia layanan IT dalam memenuhi kewajibannya.
s. Disebutkan dalam klausul pada kontrak bahwa *User* dapat melakukan audit terhadap proses, kontrol dan hasil dari aktivitas *outsourcing* yang dilaksanakan oleh penyedia layanan TI.
t. Walaupun dibuat dalam prinsip saling menguntungkan dengan kemitraan dan kolaborasi, setiap kontrak *outsourcing*, harus menyertakan kemungkinan untuk dilakukan penghentian kerjasama demi kenyamanan bersama. Dalam hal penghentian kerjasama dalam kontrak harus didefinisikan hak *User*, prosedur untuk melakukan penghentian kerjasama dan pilihan untuk membeli aset atau membayar lisensinya.
u. Operasionalisasi kebijakan ini dapat dituangkan dalam sub kebijakan pada bab selanjutnya atau pada prosedur dan standar yang mengatur secara lebih detail berkenaan dengan proses yang diperlukan dalam menyelenggarakan layanan TI.

VIII.2. Pengelolaan Layanan oleh Pihak Ketiga (Alih Daya/*Outsourcing*)

Tujuan

Kebijakan pengelolaan pihak ketiga bertujuan untuk menjamin bahwa layanan yang dijalankan oleh pihak ketiga (*suppliers*, *vendors*, dan *partners*) memenuhi kebutuhan bisnis perusahaan dan juga meminimalkan risiko bisnis jika pihak ketiga tidak dapat memenuhi kewajibannya dalam memberikan layanan TI.

Ruang Lingkup

Kebijakan ini meliputi pendefinisian tugas, tanggung jawab, dan ekspektasi dalam perjanjian dengan pihak ketiga. Demikian pula halnya dengan pendefinisan proses *reviewing* dan *monitoring* perjanjian pihak ketiga untuk pemenuhan persyaratan kepatuhan (*compliance*) terhadap aturan yang berlaku dan efektivitas layanan TI perusahaan. Disamping hal tersebut kebijakan pengelolaan layanan pihak ketiga ini harus mengatur pengelolaan risiko layanan TI oleh pihak ketiga untuk meminimalkan risiko bisnis yang berkaitan dengan apabila pihak ketiga tidak dapat memenuhi kewajibannya dalam memberikan layanan TI perusahaan. Kebijakan ini mengatur proses identifikasi hubungan pihak ketiga, *supplier relationship management*, *supplier risk management*, dan *supplier performance monitoring*.

Tanggung Jawab

a. Divisi IT bertanggung jawab untuk mengelola dan menjaga pemenuhan kinerja pihak ketiga dalam mendukung layanan yang disediakannya.
b. Setiap pegawai Danareksa wajib mengetahui setiap risiko dan konsekuensi tindakan yang dilakukannya dalam rangka keamanan jaringan ini.

Kebijakan

a. Danareksa harus memastikan bahwa pengadaan pemilihan perusahaan penyedia layanan kepada pihak ketiga telah mengikuti prosedur pengadaan barang dan jasa yang berlaku di PT. Danareksa (Persero).
b. Divisi IT harus menunjuk penanggung jawab dari internal IT Danareksa untuk mengawasi kinerja pemeliharaan atau kerjasama pengelolaan penyediaan layanan dengan pihak ketiga.
c. Untuk hal-hal tertentu dan sesuai dengan kebutuhan layanan pihak internal Danareksa, IT dapat melakukan kerja sama dengan pihak ketiga dengan bentuk kerja sama berupa "full outsource" atau berupa gabungan dari layanan internal dan eksternal.
d. Kerja sama dengan pihak ketiga di atas harus tetap menjaga tingkat kualitas layanan sesuai dengan standar kualitas layanan (SQS) yang berlaku di Danareksa.
e. Jika layanan ini berupa *outsource*, maka SLA yang diberlakukan adalah SLA *back-to-back* dari penyedia akhir layanan.

f. Jika layanan yang diberikan merupakan gabungan dari layanan internal dan eksternal, maka tingkat kualitas layanan akhir yang diberikan ke *User* adalah SLS/SLA dari pihak IT, yang merupakan gabungan dari masing-masing standar kualitas layanan yang berlaku.

g. Pada kedua jenis kerja sama di atas, tingkat kualitas layanan yang disyaratkan harus sama atau lebih baik dari standar kualitas layanan IT. Bentuk akhir perjanjian SLS/SLA yang disetujui harus memuat seluruh komponen SLS/SLA yang telah ditentukan di atas.

h. Dalam hal terjadi permintaan klarifikasi tingkat kualitas suatu layanan, maka jawaban harus diberikan oleh pihak yang memberikan layanan, baik pihak IT internal Danareksa ataupun pihak ketiga. Dalam proses selanjutnya mengenai klarifikasi tersebut apabila terjadi perselisihan, harus melibatkan atau mencapai penyelesaian yang memuaskan semua pihak internal Danareksa yang terlibat.

i. Dokumen SLS/SLA yang menyangkut pihak ketiga harus menyertakan satu atau lebih nama personil IT Danareksa dalam daftar kontak pada SLA. Personil IT yang namanya diusulkan tersebut harus ikut terlibat dalam pembicaraan, diskusi dan review mengenai SLS/SLA ini, atau segala komponen terkait lainnya seperti pelaporan dan klarifikasinya. Khusus untuk layanan yang sebagian besar bersifat TI, maka pihak IT sedapat mungkin harus menjadi titik kontak utama untuk kontrak tersebut. Komunikasi antara *User* dengan IT untuk memahami kebutuhan *User* dan solusinya.

j. Divisi IT harus memastikan bahwa layanan pihak ketiga sesuai dengan kontrak perjanjian kerjasama dan kebutuhan Danareksa dan melakukan evaluasi kinerja pihak ketiga minimal 1 (satu) bulan sebelum masa kerjasama berakhir.

k. Selama review kontrak layanan pihak ketiga, maka selalu harus diusahakan pengembangan atau perbaikan dari parameter yang digunakan untuk perhitungan kinerja. Jika perbaikan itu didapatkan, maka untuk kontrak yang sifatnya "back-to-back' dilakukan juga perbaikan SLS/SLA internal Danareksa.

l. Segala pelanggaran layanan pihak ketiga terhadap kontrak perjanjian kerjasama dengan Danareksa dapat dikenakan sanksi sesuai kontrak.

m. Semua kesepakatan terhadap penyediaan layanan dan penggunaan layanan pihak ketiga mengacu penuh kepada Hukum dan Undang-Undang yang berlaku di dalam wilayah Negara Kesatuan Republik Indonesia.

Kebijakan

Implementasi kebijakan ini dapat berupa pembuatan kontrak dengan pihak ketiga berdasarkan template kontrak yang dibuat berdasarkan persyaratan yang berlaku dalam Kebijakan ini, prosedur pengelolaan hubungan kemitraan dengan pihak ketiga, prosedur pengelolaan risiko untuk layanan pihak ketiga, dan prosedur pemantauan kinerja pihak ketiga.

IX. PENGELOLAAN KEAMANAN TEKNOLOGI INFORMASI

IX.1. Pengelolaan Sekuriti TI

Tujuan

Kebijakan ini bertujuan untuk menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi perusahaan.

Ruang Lingkup

Kebijakan pengelolaan sekuriti TI meliputi aspek-aspek tentang pendefinisian aturan sekuriti TI, yang meliputi rencana sekuriti TI, klasifikasi aset TI, prosedur sekuriti, monitoring, pendeteksian, pelaporan, penyelesaian vulnerabilities dan insiden sekuriti, serta rencana kesinambungan bisnis perusahaan *atau Business Continuity Plan* (BCP).

Note 1:

Ruang lingkup pengelolaan sekuriti TI terkait BCP adalah pada *information security* pada BCP.

Note 2:

Dalam ruang lingkup Pengelolaan Sekuriti TI adalah belum secara spesifik menyebutkan kebijakan terkait pengelolaan operasional, pengelolaan e-mail, pengelolaan *account-password*, pengelolaan antivirus (hanya ada pada bagian Kebijakan, salah satunya terkait e-mail).

Kebijakan

Pendefinisian secara lebih detail untuk kebijakan ini dapat dituangkan dalam suatu prosedur atau standar sekuriti TI yang pada umumnya mengadopsi proses Information Security Management System (ISMS) yang berbasis ISO 27000 disesuaikan dengan kebutuhan perusahaan. Salah satu standar atau *guideline* sekuriti yang umum digunakan adalah kebijakan *acceptable use of IT assets* seperti bagaimana penggunaan e-mail perusahaan, laptop perusahaan, jaringan internal perusahaan, dan hal lain yang perlu diatur pemakaiannya.

IX.2. Akses Ruang Perangkat Teknologi

Tujuan

Untuk memastikan bahwa akses terhadap ruangan dimana terdapat perangkat teknologi yang berada dalam administrasi IT hanya diberikan kepada dan dilakukan oleh mereka yang berhak dan telah mendapatkan akses tersebut sesuai dengan prosedur yang berlaku. Hal ini juga berlaku untuk meningkatkan keamanan akses terhadap informasi milik Danareksa.

Ruang Lingkup

Kebijakan ini mencakup semua ruangan perangkat teknologi yang disebutkan dalam definisi di bawah, serta semua pihak yang terlibat dan membutuhkan akses, seperti staf IT, staf unit kerja lainnya, serta pihak ketiga yang sudah diatur dalam kontrak tersendiri.

Tanggung Jawab

Divisi IT bertanggung jawab untuk menjaga akses pada ruang perangkat teknologi yang tercakup dalam lingkup kebijakan ini.

Kebijakan Keamanan

a. Semua ruang perangkat teknologi di atas harus diberikan klasifikasi “Security Zone” dan mengindahkan pengaturan tentang zona tersebut seperti pada Kebijakan Kemanan dan Keselamatan. Semua ruang perangkat teknologi harus memiliki sistem atau kontrol akses yang dapat didokumetasikan atau ditelusuri (*audit trail*) serta dipertanggungjawabkan.
b. Divisi IT harus menjaga agar sistem akses ini beroperasi secara terus menerus. Jika ada gangguan dalam sistem ini yang menyebabkan tidak berfungsinya kontrol akses, maka setiap akses oleh siapapun harus dicatatkan dalam *log book* sesuai dengan prosedur yang berlaku, dan IT wajib melaporkan serta mengusahakan perbaikan sistem kontrol akses ini secepatnya.
c. Divisi IT harus memiliki struktur dan data staf yang memiliki akses ke ruang perangkat teknologi. Pengajuan daftar akses akan dilakukan secara formal dan tercatat, serta dengan persetujuan pihak yang berwenang, dan dikelola oleh penanggung jawab ruang perangkat teknologi tersebut. Setiap perubahan atas daftar akses ini harus juga dilakukan secara formal dan tercatat.
d. Jika staf yang mempunyai akses ke ruang perangkat teknologi tidak lagi bekerja pada Danareksa, berdasarkan konfirmasi dari HC, maka secara langsung aksesnya

dibatalkan. IT harus memastikan bahwa staf yang bersangkutan tidak lagi memiliki akses ke ruang perangkat teknologi.

e. Melakukan review secara berkala terhadap daftar akses ke ruang perangkat teknologi, catatan akses (*log book*), dan catatan perubahan serta pemeliharaan yang telah berlangsung.
f. Setiap perubahan, perbaikan, penggantian yang dilakukan pada perangkat teknologi yang terdapat dalam ruang tersebut harus tercatat dalam suatu dokumentasi *change management* secara formal. Jika ada perubahan atas rencana *change management* tersebut, maka perubahan ini harus dicatatkan pada rincian kerja yang dilaporkan. Staf IT yang terlibat akan menjadi penanggung jawab dari perubahan, perbaikan dan penggantian yang dilakukan.
g. Setiap pekerjaan di atas direncanakan untuk mempunyai konsekuensi minimal terhadap kegiatan bisnis dan operasional Danareksa, misalnya pada hari libur, di luar jam operasional, dan dalam kondisi dimana seluruh sistem berada dalam keadaan *off* (*shutdown*). Pengecualian dari hal ini harus dicatatkan dalam rencana *change management*, dan disetujui oleh semua pihak terkait.
h. Rencana *change management* mensyaratkan pemberitahuan tentang pekerjaan yang dapat mengganggu operasional Danareksa minimal 5 (lima) hari kerja sebelumnya kepada semua pihak terkait. Dalam *change management* dokumen tersebut juga dicantumkan pihak IT dan pihak ketiga yang terlibat, serta akses yang diperlukan ke ruang perangkat teknologi yang ada.
i. Segala pelanggaran terhadap kebijakan dan peraturan ini dapat dikenakan sanksi seperti yang diatur pada Kebijakan Penanganan Insiden dan Sanksi, dari tindakan disipliner ringan sampai kepada tindakan pemberhentian yang bersangkutan. Sanksi ini juga dapat ditambah dengan larangan untuk melakukan akses ke ruang perangkat teknologi untuk suatu periode yang akan ditentukan nantinya.
j. Pihak ketiga yang terlibat dalam pelanggaran ini akan mendapatkan peringatan keras dari Danareksa, dengan konsekuensi lain yang diatur dalam kontrak kerja dengan pihak tersebut.

Kebijakan Keselamatan

a. Semua ruang perangkat teknologi harus memiliki sistem kontrol akses yang berfungsi, serta sistem pengaturan yang diperlukan, seperti suhu dan kelembaban, pemadam kebakaran, sesuai dengan kebutuhan perangkat teknologi yang ada di dalam ruangan tersebut. Pemeliharaan semua sistem ini sudah diatur pada Kebijakan Keamanan dan Keselamatan.

b. Untuk keadaan darurat, harus disiapkan suatu cara akses ke dalam ruang perangkat teknologi tersebut. Hal ini diperlukan jika personil yang memiliki akses sedang tidak berada di lokasi. Akses darurat ini dapat dilakukan dengan sistem *tel-key box*, yang pemakaiannya disertai berita acara oleh yang bersangkutan. Berita acara tersebut kemudian diserahkan kepada IT, yang akan melakukan pemeriksaan, dan kemudian menyediakan kembali akses *tel-key box* dengan berita acara yang baru.
c. Pihak-pihak yang terkait dengan keadaan darurat gedung wajib mengerti tata cara pemakaian akses darurat ke ruang perangkat teknologi, dan berkoordinasi dengan pihak IT.

IX.3. Kebijakan Penggunaan Jaringan Komputer

Tujuan

Untuk memastikan bahwa jaringan komputer Danareksa hanya digunakan untuk kepentingan kegiatan operasional Danareksa, sebagai sarana layanan informasi baik bagi setiap pegawai Danareksa maupun kepada pihak nasabah dan pelanggan.

Ruang Lingkup

Kebijakan ini mencakup semua jaringan baik LAN ataupun WAN yang disediakan oleh Danareksa, dan juga sambungan jaringan Danareksa ini ke jaringan-jaringan lainnya milik kantor cabang, mitra, gerai, Bursa Efek Indonesia (BEI)/Jaringan Terpadu Pasar Modal (JTPM), Bank Indonesia dan penyedia layanan lainnya.

Tanggung Jawab

a. Divisi IT bertanggung jawab untuk menjaga kinerja dan keamanan jaringan yang disediakannya.
b. Setiap pegawai Danareksa wajib mengetahui setiap risiko dan konsekuensi tindakan yang dilakukannya dalam rangka keamanan jaringan ini. IT melakukan sosialisai perihal risiko tersebut kepada pegawai Danareksa.

Kebijakan

a. Kebijakan LAN

i. LAN sebagai jaringan terbatas digunakan oleh Danareksa untuk mendukung kegiatan para pemakai komputer dan aplikasi Danareksa, termasuk aplikasi *front-office*, aplikasi *back-office*, aplikasi akuntansi dan aplikasi standar Danareksa

lainnya.

ii. Akses ke LAN Danareksa didapatkan jika pegawai Danareksa mendapatkan akses ke komputer Danareksa. Pegawai Danareksa tidak diperbolehkan melakukan akses ke LAN dengan cara lainnya.

iii. Pihak IT wajib memiliki daftar akses ke LAN, dengan cara memiliki daftar alokasi komputer kepada pegawai Danareksa, dan akses khusus oleh pihak ketiga, atau daftar *network account* yang masih berlaku. Akan dilakukan *review* secara periodik terhadap daftar akses ke LAN ini.

iv. Jika staf yang mempunyai akses LAN tidak lagi bekerja pada Danareksa, berdasarkan konfirmasi dari Divisi Human Capital (HC), maka secara langsung aksesnya dibatalkan. IT harus memastikan bahwa staf yang bersangkutan tidak lagi memiliki akses ke komputer ataupun LAN Danareksa, terhitung satu hari kerja setelah hari kerja terakhir.

v. Jika ada pihak ketiga yang melakukan akses ke LAN Danareksa, misalnya dengan menggunakan perangkat komputernya sendiri, maka hal ini harus dilakukan setelah ada persetujuan dari IT. Pihak internal Danareksa yang terkait dengan pihak ketiga ini dapat melakukan permohonan akses ini kepada IT. Pada pihak ketiga ini akan berlaku kebijakan akses pihak ketiga yang diatur tersendiri.

vi. Danareksa tidak memperbolehkan komputer ataupun perangkat teknologi milik Danareksa lainnya, ataupun perangkat yang dipasang oleh pihak ketiga dalam LAN Danareksa, untuk langsung tersambung ke jaringan komputer lainnya pada waktu yang bersamaan. Contohnya, komputer yang tersambung ke jaringan milik penyedia layanan *real time* (RTI) tidak boleh langsung tersambung ke LAN Danareksa, atau komputer Danareksa tersambung ke LAN Danareksa dan sekaligus langsung tersambung ke Internet. Jika pihak internal Danareksa membutuhkan sambungan khusus seperti di atas, harus dilakukan sepengetahuan dan atas persetujuan IT.

vii. Jaringan komputer milik perusahaan lainnya yang terafiliasi, harus menempati segmen yang berbeda dengan segmen yang digunakan untuk operasional Danareksa.

viii. Untuk pengamanan tambahan LAN Danareksa antar segmen tersebut di atas, maka Danareksa menggunakan perangkat *firewall* dan IDS pada tingkat *backbone*.

ix. Kabel dan *connector* (RJ45) yang digunakan untuk menghubungkan antar peralatan komunikasi data atau komputer harus disesuaikan dengan kode warna yang digunakan dan minimal menggunakan kabel UTP *category* 6.

x. *Backbone* yang menghubungkan jaringan komputer pada tiap lantai secara minimum harus terdiri dari 4 kabel Fiber Optik, dan 4 kabel UTP (*Unshielded Twisted Pair*) minimal *category* 6 (2 *backbone live* dan 2 *backbone* sebagai

backup kabel FO).

b. Kebijakan WAN

i. WAN sebagai jaringan terbatas digunakan Danareksa untuk menghubungkan lokasi Danareksa, dan dengan kantor cabang, mitra, serta gerai Danareksa. Sedapat mungkin jaringan WAN ke kantor cabang, mitra dan gerai menggunakan jaringan WAN yang telah ada.

ii. Jaringan komputer pada mitra atau gerai sebagai sarana untuk melakukan transaksi tidak diperbolehkan terhubung dengan jaringan Danareksa lain dan sekaligus langsung ke internet. Secara keseluruhan, kebijakan keamanan informasi di lokasi mitra/gerai akan diatur dalam perjanjian kerjasama tersendiri.

iii. Jaringan yang terhubung ke jaringan WAN Danareksa harus melakukan pengamanan dan pengawasan yang sama dengan yang dilakukan Danareksa. Semua kebijakan keamanan informasi yang berlaku di Danareksa harus juga di-aplikasikan ke jaringan lainnya yang tersambung ke jaringan Danareksa. Contoh: jaringan mitra atau gerai juga mempunyai perlindungan yang sama (*Firewall*, IDS, *access control*, *software antivirus*) dengan yang digunakan di jaringan Danareksa.

iv. Danareksa berhak ikut melakukan pengawasan atau audit pada jaringan mitra atau gerai yang terhubung secara langsung ke jaringan Danareksa. Hal ini akan diatur dalam perjanjian kerja sama dengan pihak mitra atau gerai tersebut. Kegiatan audit itu sendiri akan diatur langsung oleh Divisi Internal Audit Danareksa.

v. Terbuka kemungkinan Danareksa melakukan sambungan WAN ke jaringan lainnya dengan menggunakan perangkat *firewall* pada daerah batas. *Firewall* dan daerah batas ini digunakan untuk secara fisik dan kebijakan memisahkan jaringan Danareksa dengan jaringan lain tersebut. Dalam hal ini hak dan kewajiban untuk memelihara jaringan berada di masing-masing pihak, dengan persetujuan bahwa kedua belahpihak akan saling tukar-menukar informasi yang dibutuhkan untuk saling mengamankan jaringan masing-masing, serta mengamankan transaksi atau pertukaran informasi yang terjadi.

c. Kebijakan Akses *Remote*

i. Akses *remote* ke jaringan Danareksa harus aman dan di kontrol secara ketat dengan perlindungan enkripsi ((misalnya, *Virtual Private Network* (VPN)) dan penggunaan *Dual* (*split*) *tunneling* TIDAK diizinkan.

ii. Pengguna hak *remote* akses seperti pegawai Danareksa, tenaga kontrak, konsultan, mitra, vendor atau pihak ketiga lainnya harus menyadari bahwa

koneksi *remote* akses yang diberikan sama seperti penggunaan koneksi di dalam jaringan Danareksa dengan demikian akan mengikuti segala ketentuan dan peraturan yang berlaku di Danareksa.

iii. Ketika mengakses jaringan Danareksa dari perangkat komputer luar, pengguna *remote* akses harus memastikan perangkat yang digunakan aman bersih dari virus, *malware* dan program jenisnya, serta menggunakan *software* antivirus dan definisi virus yang paling *up-to-date*.

iv. Pengguna *remote* akses harus melindungi *login* dan *password* mereka serta bertanggung jawab dari penyalahgunaan hak akses atau kegiatan illegal lainnya yang dapat mengganggu kepentingan bisnis Danareksa.

v. Pengguna *remote* akses akan secara otomatis terputus dari jaringan Danareksa setelah tiga puluh (30) menit tidak aktif. Pengguna kemudian harus *log on* lagi untuk menyambung kembali ke jaringan. *Ping* atau proses jaringan buatan lainnya tidak boleh digunakan agar jaringan tetap terhubung.

d. Kebijakan Nirkabel (*Wireless*)

i. Akses *wireless* saat ini diberlakukan sebagai jalur komunikasi khusus untuk internet dimana semua perangkat yang dipasang tidak terhubung langsung ke jaringan Danareksa.

ii. Penggunaan semua perangkat jaringan nirkabel harus menerapkan pengamanan infrastruktur, protokol otentifikasi dan enkripsi yang disetujui dan terbukti aman.

iii. Perangkat *wireless* Danareksa di-*install*, didukung dan dikelola oleh tim infrastruktur IT yang secara periodik melakukan perubahan otentifikasi akses (misalkan, WPA-PSK pada *access point* Wifi). Pemeliharaan terhadap perangkat *wireless* tidak boleh dilakukan oleh vendor atau pihak ketiga.

iv. Jika dibutuhkan koneksi nirkabel antara jaringan Danareksa dan jaringan eksternal, maka diberlakukan juga aturan seperti pada kebijakan dengan pihak ketiga.

IX.4. Penggunaan Jaringan Telekomunikasi

Tujuan

Untuk memastikan bahwa jaringan telekomunikasi yang ada, dan perangkat yang disediakan, hanya diberikan kepada dan diakses oleh mereka yang berhak sesuai dengan kewenangan akses yang diberikan.

Ruang Lingkup

Kebijakan ini mencakup semua sarana telekomunikasi yang disediakan oleh Danareksa, seperti telepon, fax, dan telepon genggam, serta semua pegawai Danareksa yang mendapatkan akses penggunaan sarana ini.

Tanggung Jawab

a. Divisi IT bertanggung jawab untuk memelihara atau mengelola daftar akses sarana telekomunikasi dan melakukan setiap perubahan yang sudah disetujui.
b. Setiap pegawai Danareksa wajib mengindahkan dan mengikuti peraturan yang diberlakukan sehubungan dengan akses ke sarana telekomunikasi, dan wajib mengetahui setiap risiko dan konsekuensi tindakan yang dilakukannya dalam menggunakan sarana ini. Danareksa berhak untuk melakukan perekaman penggunaan perangkat telekomunikasi tersebut, yang akan didokumentasikan sesuai dengan kebijakan Danareksa, dan dapat digunakan di kemudian hari sebagai bukti pendukung.

3.1. Kebijakan

a. Jaringan telekomunikasi didefinisikan sebagai jaringan berbasis suara (*voice-based*), yaitu telepon dan fax. Danareksa telah melakukan instalasi jaringan telekomunikasi internal untuk setiap pegawai Danareksa, dan juga telah melakukan koneksi dengan pihak penyedia layanan nasional untuk memungkinkan pegawai Danareksa berkomunikasi dengan pihak eksternal untuk kepentingan kegiatannya.
b. Setiap pegawai Danareksa dapat dialokasikan minimal satu buah saluran telepon. Setiap penggunaan sarana komunikasi ini untuk keperluan menghubungi pihak eksternal dicatat dalam aplikasi *billing* telepon yang disediakan oleh Danareksa. Pemakaian atau pembatasan penggunaan telepon ini diatur tersendiri melalui keputusan direksi.
c. Pihak IT mencatat daftar pegawai yang memiliki akses untuk menggunakan sarana telekomunikasi ini. Setiap perubahan pada daftar akses ini akan dilakukan berdasarkan permintaan yang formal dan tercatat. Jika ada pegawai Danareksa yang mempunyai akses telekomunikasi yang tidak lagi bekerja pada Danareksa, dengan konfirmasi dari HC, maka secara langsung aksesnya dibatalkan. IT harus memastikan bahwa staf yang bersangkutan tidak lagi memiliki akses telekomunikasi yang dimaksud terhitung satu hari kerja setelah hari kerja terakhir bagi yang bersangkutan.

d. IT wajib memiliki daftar pegawai Danareksa yang memperoleh alokasi perangkat telekomunikasi. Setiap perubahan atas daftar ini harus dilakukan secara formal dan tercatat.
e. Setiap pegawai wajib menjaga akses sarana telekomunikasi yang dimilikinya, dalam bentuk PIN atau *password*. Setiap pegawai bertanggung jawab atas akses sarana telekomunikasi yang dilakukan dengan *password* atau PIN yang dimilikinya.
f. Jika Danareksa mendeteksi adanya pemakaian yang tidak wajar atas sarana telekomunikasi ini, Danareksa dapat melakukan pemeriksaan terhadap pemakaian ini, termasuk terhadap pegawai yang memiliki PIN atau *password* termaksud.
g. Danareksa dapat melakukan perekaman atas pembicaraan yang dilakukan, terutama dalam operasional transaksi oleh *Sales*/*Account Executive*/Agen/transaksi *dealing room* Danareksa. Catatan perekaman ini akan disimpan sesuai dengan peraturan perundangan yang berlaku.
h. Konfigurasi jaringan telekomunikasi Danareksa memberikan saluran kepanjangan (*extension*) kepada setiap kantor cabang Danareksa, sesuai dengan kebutuhan kantor cabang yang bersangkutan, dan ketersediaan peralatan teknologi yang diperlukan. Setiap komunikasi internal antar kantor sedapat mungkin dilakukan dengan menggunakan saluran kepanjangan ini.
i. Danareksa menyediakan fasilitas *conference* yang dapat digunakan oleh setiap divisi sesuai dengan kapasitas yang ada. Setiap divisi/bagian Danareksa mempunyai nomor bagian yang dapat digunakan untuk layanan *conference* ini.
j. Danareksa menyediakan layanan faksimil kepada setiap unit Danareksa. Layanan ini dapat bersifat terpusat ataupun secara per bagian, yang akan diatur secara tersendiri.
k. Segala pelanggaran terhadap kebijakan dan peraturan ini dapat dikenakan sanksi seperti yang diatur pada Kebijakan Penanganan Insiden dan Sanksi, dari tindakan disipliner ringan sampai kepada tindakan pemberhentian yang bersangkutan.

IX.5. Penggunaan *Server*

Tujuan

Untuk memastikan bahwa keamanan perangkat sistem *server* dan *storage* dikelola dengan baik dan hanya diberikan akses oleh mereka yang berhak sesuai dengan kebijakan yang berlaku.

Ruang Lingkup

Kebijakan ini mencakup semua sarana *server* dan *storage* yang disediakan oleh Danareksa serta pengelolaan perangkat Danareksa oleh pegawai yang mendapatkan akses sarana ini.

Tanggung Jawab

Pihak IT wajib memelihara dan menjaga perangkat *server* dan *storage* agar selalu berfungsi secara handal serta mengatasi segala gangguan operasional yang terjadi atas perangkat tersebut.

Kebijakan

a. Semua *server* dan *storage* yang digunakan di internal Danareksa dikelola oleh Divisi IT dan menjadi tanggung jawab sistem administrator, dimana operasional pemeliharaan, konfigurasi dan pengawasan dilakukan sesuai standar TI dan kebutuhan bisnis. Pemakai non administrator dilarang mengakses perangkat *server* langsung atau secara *remote*.
b. Sistem Administrator harus memiliki daftar inventaris semua perangkat *server* dan *storage* (*Physical* dan *Virtual*) yang tetap *up-to-date*, setiap perubahan komponen ataupun konfigurasi perangkat produksi harus selalu terdokumentasi.
c. Perangkat *server* dan *storage* secara fisik harus berada diruang khusus perangkat TI dengan akses khusus sesuai kebijakan Akses Ruang Peralatan Teknologi. Perangkat *server* harus menggunakan *antivirus*, *spyware*, *patch* keamanan terbaru atau fitur keamanan lain, kecuali mengganggu aplikasi atau kebutuhan bisnis.
d. Semua yang berhubungan dengan keamanan pada sistem server produksi kritikal atau sensitif harus mengaktifkan *log* keamanan, *audit trails* dan di-*backup log* secara periodik, hal ini dapat digunakan untuk pemantauan keamanan, perbaikan atau investigasi permasalahan.
e. Ketersediaan layanan *server* dan *storage* dijaga sesuai standar layanan infrastruktur IT, sistem produksi harus memiliki perangkat *backup* dan pemeliharaan oleh tenaga ahli atau vendor untuk mengurangi resiko terhadap kemungkinan gangguan.

IX.6. Penggunaan *Password*

Tujuan

Untuk menjaga akses ke sistem dan informasi yang tersedia di Danareksa hanya kepada mereka yang berhak, dan untuk mencegah terjadinya kerusakan, kehilangan, kebocoran data ataupun informasi yang berasal dari akses oleh pihak-pihak luar secara tidak semestinya.

Ruang Lingkup

Kebijakan ini berlaku pada semua *user account* yang digunakan dalam lingkup Danareksa.

Tanggung Jawab

a. *Password* sistem dan *software* Danareksa setingkat administrator menjadi tanggung jawab internal IT.
b. *Password* setingkat akses *User* menjadi tanggung jawab setiap pegawai yang di-*assign*, termasuk semua aktivitas dan transaksi yang dibuat dengan *username* dan *password* tersebut.
c. Unit/Divisi/*User* terkait yang memberikan izin penggunaan *password* kepada pihak ketiga bertanggung jawab untuk menjaga penggunaan *username* dan *password* untuk pihak ketiga yang telah mendapatkan ijin untuk menggunakan *username* dan *password* di lingkungan Danareksa. Danareksa mendelegasikan tanggung jawab ini kepada unit kerja yang terkait dengan pihak ketiga yang bersangkutan.

Kebijakan

a. Setiap pegawai Danareksa wajib menggunakan *username* dan *password* yang telah diberikan dan menjadi tanggung jawab mereka untuk mengakses komputer, data dan informasi yang mereka gunakan.
b. Semua pegawai bertanggung jawab atas segala aktivitas yang dilakukan dalam sistem ataupun *software* Danareksa yang menggunakan *username* dan *password* yang di-*assign* kepadanya.
c. Setiap pemilik *username* pada sistem wajib untuk memelihara kerahasiaannya *password*-nya, dan mengganti *password* tersebut secara periodik, berdasarkan aturan yang telah ditetapkan, misalnya seperti pada huruf (d) di bawah ini.
d. Semua *password* yang dimiliki oleh *User* (misalnya, e-mail, *desktop computer*, *web*, aplikasi dan lain-lain) harus paling tidak memenuhi persyaratan sebagai berikut:

    i. Panjang minimum = 8 karakter
    ii. Batas maksimum periode penggantian *password* = 180 hari
    iii. Batas minimum periode penggantian *password* = 1 hari
    iv. *Password history* = 6
    v. Setiap *password* harus merupakan kombinasi komplek, setidaknya terdiri dari huruf *alphabet*, angka dan simbol seperti karakter sebagai berikut:

!@#$%A&*()_

e. Untuk pegawai yang baru mendapatkan *username* dan *password* untuk akses ke sistem yang diperlukannya, maka pegawai wajib langsung mengganti *password* yang diterimanya dengan suatu kombinasi seperti yang diatur di atas, yang hanya diketahui olehnya. Pegawai tidak boleh menggunakan *password* yang berupa *default* dari sistem ataupun *software* yang bersangkutan, ataupun *password default* yang diberikan dari pihak IT.
f. Semua *password* harus langsung diganti, baik oleh pegawai yang bersangkutan ataupun dilaporkan kepada dan kemudian diganti oleh IT, jika dicurigai adanya ketidakamanan *username* ataupun *password* termaksud.
g. Jika terjadi 3 kali pegawai salah memasukkan *username* dan *password*-nya, maka *username* yang bersangkutan akan langsung berstatus ”suspended” atau ”disabled”. Pegawai harus melaporkan ke IT/Helpdesk untuk mengaktifkan kembali *password*-nya.
h. Pihak eksternal dapat memperoleh akses dengan level ”Guest” pada sistem Danareksa. Apabila pihak tersebut memerlukan akses di atas ”Guest” maka harus menyertakan permintaan dari Divisi *counterpart*-nya di Danareksa dan mendapatkan persetujuan dari tingkat Kepala Divisi.

i. Jika pegawai mengundurkan diri, maka *account* yang bersangkutan akan ”disabled” satu hari setelah tanggal kerja terakhir pegawai tersebut, berdasarkan konfirmasi dari HC. Setelah itu *account* yang bersangkutan akan dihapus dari semua sistem dimana *account* tersebut berada minimal 1 (satu) hari dan maksimal 7 hari setelah tanggal keluarnya pegawai tersebut kecuali ada permintaan khusus dari Direksi atau Kepala Unit/Kepala Divisi yang bersangkutan.
j. Semua *password* harus diperlakukan sebagai informasi rahasia yang sensitif, pegawai harus melindungi pengguaan *username* dan *password* dengan sekurang-kurangnya melakukan hal berikut ini:

    i. Tidak berbagi atau memberikan *password* kepada orang lain, termasuk asisten administrasi, sekretaris, manajer, rekan kerja saat berlibur atau anggota keluarga.
    ii. Tidak mencatat atau menuliskan *password* secara jelas dan dapat terlihat oleh orang lain, misalnya pada “Post-It Notes”, file, e-mail, ponsel ataupun media lainnya.
    iii. Jangan menggunakan fitur aplikasi “Remember Password”, misalnya pada aplikasi *web browser*.

iv. Tidak menggunakan *password* yang sama untuk beberapa *account*, misalnya untuk e-mail, aplikasi, web, dan sebagainya.

k. Jika pegawai mendapati perlakuan terhadap *password* yang tidak semestinya yang dilakukan oleh sejawatnya, maka pegawai wajib memberitahu yang bersangkutan agar mematuhi kebijakan Danareksa mengenai *password*. Jika pemberitahuan tersebut tidak diindahkan, maka pegawai wajib meneruskan informasi ini kepada manajer yang bersangkutan, dan sekaligus kepada pihak IT/Helpdesk.

l. Jika dalam pemeriksaan didapatkan bukti bahwa user yang bersangkutan telah menyalahgunakan *username* dan *password* yang dimilikinya atau perlakukan terhadap *password*-nya melanggar kebijakan Danareksa yang telah ditetapkan, maka akan dibebankan sanksi administratif seperti yang diatur pada Kebijakan Penanganan Insiden dan Sanksi.

m. Pihak IT menyimpan daftar akses penguna sistem informasi dan melakukan review secara periodik dengan berkoordinasi dengan pihak HC. Pada daftar akses ini dimungkinkan pembatasan lebih lanjut seperti sistem yang dapat diakses, serta waktu, cara, dan lokasi akses.

n. IT harus melindungi setiap perangkat informasi yang harus dibatasi aksesnya, misalnya perangkat *Switch*, *Router*, *Firewall* dan *File Server*. Untuk setiap sistem perangkat diatur pembagian aksesnya, termasuk terhadap penanggung jawab dan administratornya.

o. Untuk setiap aplikasi Danareksa, Kepala Unit dimana mayoritas pengguna berada wajib menunjuk satu orang administrator *User Account* yang bertugas untuk mengatur akses para pengguna aplikasi tersebut. Segala perubahan terhadap daftar akses ini dilakukan secara formal dan tercatat.

p. *Username* dan *password* yang setingkat dengan administrator sistem ataupun *software* Danareksa (sseperti *root*, *enable*, *domain admin*, *application administration accounts*, dan lainnya), yang dimiliki oleh personil dalam grup IT, harus memenuhi persyaratan *password* yang kuat, sebagai berikut:

i. Panjang minimum = 12 karakter

ii. Batas maksimum periode penggantian *password* = 90 hari

iii. Batas minimum periode penggantian *password* = 1 hari

iv. *Password history* = 12

v. Setiap *password* harus merupakan kombinasi komplek, setidaknya terdiri dari huruf alphabet, angka dan simbol seperti karakter sebagai berikut: !@#$%^&*()_

q. Semua *password* administrator sistem akan disimpan masing-masing dalam sebuah amplop tertutup, dan *account* dengan akses setara administrator akan diberikan kepada masing-masing personil yang membutuhkannya. Personil tersebut dilarang untuk menggunakan *accoun*t ini untuk keperluan sehari-harinya, dan hanya akan menggunakannya untuk akses ke sistem *server* TI.
r. Dalam keadaan darurat, dimungkinkan untuk membuka amplop *password* admin di atas dan menggunakannya setelah mengisi berita acara yang terlampir secara lengkap. Berita acara tersebut kemudian diserahkan kepada IT, yang akan melakukan pemeriksaan, dan kemudian menyediakan kembali akses dengan *password* administrator dan berita acara yang baru.
s. Segala pelanggaran terhadap kebijakan dan peraturan ini dapat dikenakan sanksi seperti yang diatur pada Kebijakan Penanganan Insiden dan Sanksi, dari tindakan disipliner ringan sampai kepada tindakan pemberhentian yang bersangkutan.

Pedoman *Password*

Password yang kuat memiliki karakteristik sebagai berikut:

a. Mengandung setidaknya 12 karakter alfanumerik.
b. Mengandung kedua huruf besar dan huruf kecil.
c. Mengandung setidaknya satu angka (misalnya, 0-9).
d. Mengandung setidaknya satu karakter khusus, misalnya, $%^&*()_+|~- =\`{}:";'<,/!?).

Password memiliki karakteristik lemah sebagai berikut:

a. Mengandung kurang dari (8) delapan karakter.
b. Dapat ditemukan dalam kamus, termasuk bahasa asing, atau ada dalam bahasa gaul, dialek, atau jargon.
c. Mengandung informasi pribadi seperti tanggal lahir, alamat, nomor telepon, atau nama anggota keluarga, binatang peliharaan, teman, dan karakter fantasi.
d. Mengandung informasi yang berhubungan dengan pekerjaan seperti nama bangunan, perintah sistem, situs, perusahaan, *hardware*, atau perangkat lunak.
e. Mengandung pola nomor seperti aaabbb, qwerty, zyxwvuts, atau 123.321.
f. Mengandung kata-kata umum dieja mundur, atau didahului atau diikuti dengan nomor (misalnya: terces, secret1 atau 1secret).
g. Beberapa versi *password* lemah "Welcome123" "password123" "Changeme123" ,Sebaliknya membuat *password* yang dapat diingat dengan mudah, misalnya dengan membuat *password* berdasarkan judul lagu, penegasan, kalimat atau frase. Contohnya : "In1 c4r4 mud4h m*nging4t", “h4r1M3rdeka$”, “di74lan $3dan6 B4njir” atau variasi lain. Catatan: Jangan gunakan contoh diatas sebagai *password*!

IX.7. Penggunaan E-mail

Tujuan

Untuk menjaga agar penggunaan fasilitas e-mail Danareksa adalah hanya untuk kepentingan Danareksa.

Ruang Lingkup

Kebijakan ini berlaku pada semua pegawai pengguna fasilitas e-mail Danareksa.

Tanggung Jawab

a. Divisi IT bertanggung jawab atas kinerja, ketersediaan, dan keamanan fasilitas e-mail Danareksa.
b. Divisi IT bertanggung jawab untuk melakukan pemeriksaan periodik ataupun insidental terhadap fasilitas e-mail Danareksa.
c. Setiap pegawai bertanggung jawab atas semua e-mail yang terkirim dari *account*-nya masing-masing, sehingga kewajiban pengamanan *account* termaksud juga menjadi tanggung jawab setiap pegawai.

Kebijakan

a. Fasilitas e-mail Danareksa harus digunakan untuk kepentingan dan kegiatan Danareksa, serta penggunaannya tidak bertentangan dengan peraturan Danareksa maupun peraturan perundangan yang berlaku.
b. Pada pegawai Danareksa dapat diberikan akses ke e-mail Danareksa melalui *web interface* dengan persetujuan Kepala Unit pegawai tersebut.
c. Penggunaan fasilitas e-mail Danareksa untuk kepentingan pribadi pegawai masih dapat ditoleransi sampai satu tingkat dimana kepentingan Danareksa tidak dirugikan atau dikesampingkan.
d. Monitoring fasilitas e-mail dapat dilakukan secara periodik atau acak, dimana dipandang perlu dan tanpa pemberitahuan sebelumnya. Danareksa dapat memberi hak kepada staf tertentu untuk melakukan pemeriksaan fasilitas e-mail ini dan penggunaannya oleh pegawai Danareksa.
e. Secara berkala akan dilakukan audit pada fasilitas e-mail Danareksa oleh pihak internal maupun eksternal, dengan tujuan untuk memastikan bahwa fasilitas termaksud tetap dapat mendukung kegiatan Danareksa secara aman dan andal.

f. Semua pesan e-mail yang dikirim maupun diterima melalui fasilitas e-mail Danareksa menjadi hak dan milik Danareksa.
g. Danareksa mempunyai hak untuk membatasi ukuran penyimpanan e-mail untuk pegawai. Diharapkan semua pegawai melakukan pemeliharaan kapasitas e-mail mereka secara periodik atau dimana diperlukan.
h. Untuk kepentingan kegiatan internal Danareksa, segala perjanjian yang dituangkan melalui fasilitas email Danareksa bersifat tetap dan mengikat secara peraturan, setara dengan dokumen tertulis. Catatan bisnis Danareksa harus dipertahankan sesuai standar kebijakan retensi data perusahaan.
i. Standar penggunaan dan penulisan e-mail Danareksa harus bersifat sopan dan profesional, sesuai dengan standar yang digunakan untuk komunikasi dengan media lainnya. Fasilitas email Danareksa tidak boleh digunakan untuk hal-hal yang menyinggung orang lain, yang berkenaan dengan politik, SARA, asusila, fitnah, dan lain-lain.
j. Pegawai hanya menggunakan fasilitas e-mail Danareksa untuk mengirimkan informasi yang relevan untuk penerima yang dituju. Penggunaan ”Reply To All” harus dijaga agar sirkulasi informasi dibatasi kepada mereka yang berkepentingan saja.
k. Pegawai harus memastikan terlebih dahulu bahwa penerima e-mail tersebut adalah benar-benar mereka yang dituju, untuk sangat meminimalkan risiko salah penerimaan karena kemiripan alamat e-mail ataupun kemungkin mengandung *malware*. Hal ini harus dilakukan baik untuk e-mail kepada sesama pegawai Danareksa, e-mail yang bersifat sensitif, ataupun yang menyangkut pihak eksternal.
l. Jika pegawai berhalangan dari kegiatan Danareksa untuk waktu yang cukup lama, misalkan karena cuti, diharapkan menggunakan fasilitas ”Out of Office” yang telah disediakan untuk Danareksa. Jika yang bersangkutan telah kembali aktif di Danareksa, maka fasilitas di atas harus kembali di non-aktifkan.
m. Pegawai diharapkan mengefektifkan penggunaan e-mail, seperti menjaga e-mail sesingkat mungkin, penggunaan *Subject* yang jelas, *signature* yang informatif pada bagian akhir e-mail.
n. Pegawai bertanggung jawab atas e-mail yang dikirimkan dari *account* mereka. Pegawai harus berusaha untuk menjaga fasilitas e-mail yang disediakan untuk mereka, dalam hal keamanan dan perlindungan informasi. Jika pegawai meninggalkan komputernya untuk waktu yang lama, maka layar komputer tersebut harus diproteksi dengan *password* (*screen saver*).
o. Pegawai diharuskan untuk melaporkan kepada manager mereka atau kepada IT jika mereka menemukan penggunaan email yang melanggar peraturan kebijakan ini.

p. Pegawai dilarang mengirimkan e-mail berupa surat berantai ataupun sejenisnya. Pegawai juga dilarang menggunakan fasilitas e-mail Danareksa untuk mengirimkan e-mail dalam jumlah besar (SPAM), yang isinya tidak berkaitan dengan bisnis Danareksa atau melanggar etika dan peraturan yang ada. Pegawai akan dianggap bertanggung jawab atas satu pelanggaran serius jika SPAM yang dikirimkannya mengakibatkan sistem e-mail Danareksa di-*block* oleh otoritas Internet.
q. Pegawai harus sangat hati-hati saat mengirim e-mail dari Danareksa ke jaringan eksternal dan dilarang meneruskan secara automatis "Auto Forward" e-mail Danareksa yang mengandung informasi rahasia atau sensifif dari Danareksa ke sistem e-mail pihak ketiga.
r. IT hanya akan menjaga e-mail dalam masa transit di *server*. E-mail yang sudah di-*download* oleh pegawai ke komputernya menjadi tanggung jawab pegawai sepenuhnya.
s. E-mail yang berisi informasi sensitif harus ditandai sebagai *confidential*, e-mail tersebut harus dikirimkan secara terproteksi atau enkripsi.
t. E-mail yang dikirim dengan fasilitas e-mail Danareksa kepada pihak eksternal harus memuat DISCLAIMER standar yang telah ditetapkan Danareksa. Adapun pemuatan DISCLAIMER ini akan diatur melalui sistem untuk meminimalkan kesalahan yang dapat terjadi.
u. Pegawai tidak diijinkan menggunakan fasilitas e-mail Danareksa untuk mendapatkan informasi ataupun material yang bersifat ilegal atau melanggar hukum. Tindakan ini merupakan pelanggaran serius dengan risiko sanksi administratif dan disipliner seperti yang diatur pada Kebijakan Penanganan Insiden dan Sanksi.
v. Mengakses ataupun penggunaan e-mail dengan *user account* milik orang lain tanpa sepengetahuan pemiliknya merupakan pelanggaran serius dengan risiko sanksi administratif dan disipliner.
w. Danareksa memiliki hak penuh untuk mencabut atau melarang kegiatan-kegiatan yang bersifat pribadi yang menggunakan fasilitas e-mail Danareksa, dimana dipandang sudah terjadi penyalahgunaan fasilitas tersebut. Keputusan pencabutan, penghapusan, atau pelarangan hak ini berada pada Manager pegawai yang bersangkutan, dan atau pada IT. Untuk setiap penyalahgunaan ini dapat diberikan sanksi administratif maupun disipliner.
x. Segala pelanggaran terhadap kebijakan dan peraturan ini dapat dikenakan sanksi, dari tindakan disipliner ringan sampai kepada tindakan pemberhentian yang bersangkutan.

IX.8. Penggunaan *Antivirus*

Tujuan

Untuk menjaga sistem komputer yang digunakan di Danareksa, baik pada level *server* maupun pada level *User*, terbebas dari serangan virus.

Ruang Lingkup

Kebijakan ini berlaku pada semua perangkat komputer baik PC maupun *notebook* yang secara rutin tersambung ke *network* Danareksa, dan semua *server* Danareksa. Kebijakan ini juga mencakup sistem komputer yang berhubungan langsung dengan Internet, seperti HTTP, SMTP, FTP, DNS, dan sistem lainnya.

Tanggung Jawab

a. Semua pegawai Danareksa bertanggung jawab atas perlindungan terhadap virus untuk perangkat komputer yang dipakainya untuk tugas sehari-hari.
b. IT bertanggung jawab atas perlindungan terhadap virus untuk semua perangkat *server* Danareksa dan sistem komputer yang berhubungan langsung dengan Internet. IT juga bertanggung jawab untuk menyiapkan *update antivirus engine* dan *virus definition file* yang akan digunakan untuk *update* bagi pengguna komputer lainnya di Danareksa.

Kebijakan

a. Seluruh sistem komputer yang digunakan di Danareksa harus memiliki perlindungan yang cukup terhadap serangan virus, dalam bentuk *software* anti virus yang terinstall dan aktif. *Software* antivirus yang aktif artinya *software* tersebut senantiasa menjaga komputer dari serangan virus baru, dan secara periodik mendapatkan *update file* definisi virus terbaru.
b. Selain dari itu, *software* antivirus yang aktif secara periodik, sekali seminggu, melakukan *scanning* terhadap semua *file* lokal yang tersimpan.
c. *Software* antivirus yang aktif mempunyai dua komponen yang harus senantiasa mendapatkan *update software engine* dan virus *definition file*. Pihak IT wajib melakukan setup awal pada komputer Danareksa untuk memastikan *software* tersebut akan mendapatkan kedua jenis *update* ini. IT harus dapat membuat daftar komputer-komputer yang tidak mendapatkan kedua jenis *update* di atas, dan melakukan verifikasi dan konfigurasi langsung pada komputer-komputer tersebut.
d. Jika pegawai Danareksa mencurigai ada *file* atau perangkat IT yang mengalami serangan virus, pegawai tersebut harus memberitahukannya langsung kepada IT, serta mengusahakan perangkat tersebut tidak tersambung ke jaringan atau dimatikan sampai perangkat tersebut diverifikasi bebas dari virus.

e. Perangkat-perangkat penyimpan *file* seperti *e-mail attachment*, *external disk*, *removable device* atau lainnya harus di-*scan* terlebih dahulu dengan *software* antivirus yang ter-*install* sebelum dipergunakan di komputer Danareksa.
f. Pegawai yang menggunakan *notebook* atau *mobile computer* (*smartphone*), wajib melakukan *scan* pada *file-file* yang ditransfer ke *network* Danareksa, atau pada saat *notebook* yang digunakan disambungkan ke *network* Danareksa. Jika ada keraguan mengenai masih ada atau tidaknya virus pada perangkat di atas, pegawai wajib melaporkannya kepada IT sebelum perangkat yang bersangkutan disambungkan ke *network* Danareksa.
g. Tamu atau pihak eksternal tidak diperbolehkan untuk tersambung ke jaringan Danareksa tanpa ijin terlebih dahulu. Pihak penerima tamu tersebut di Danareksa wajib memastikan bahwa komputer yang akan tersambung bebas dari virus. Jika terdapat keraguan, IT berhak untuk menolak menyambungkan perangkat eksternal tersebut ke jaringan Danareksa.
h. Pegawai dilarang menggunakan *software P-to-P* untuk *download* dari Internet atau sumber eksternal lainnya. Pegawai harus tetap waspada akan kemungkinan terserang virus/*spyware*/trojan/*back door* lainnya karena *download* ataupun meng-*install software* yang berasal dari Internet.
i. Jika pegawai baik sengaja ataupun tidak ikut menyebarkan virus/*spyware*/Trojan/*back door*/*spam* dan lainnya, hal ini dapat dianggap sebagai pelanggaran serius dengan sanksi administratif dan disipliner seperti yang diatur pada Kebijakan Penanganan Insiden dan Sanksi.

IX.9. Penggunaan *Software*

Tujuan

Kebijakan ini mencakup penggunaan *software original* dan standar yang telah ditetapkan oleh Danareksa dan juga *software* lainnya yang digunakan oleh pegawai Danareksa sesuai dengan kebutuhan. Penggunaan yang diatur dalam kebijakan ini adalah penggunaan yang sesuai dengan strategi Danareksa, dengan *license agreement* masing-masing *software* yang digunakan, dan juga sesuai dengan peraturan perundangan yang berlaku.

Ruang Lingkup

Kebijakan ini mencakup penggunaan seluruh *software* yang ter-*install* dalam komputer Danareksa, termasuk OS (*server* dan *workstation*), *Office application*, *antivirus* (*server* dan *workstation*), *software platform* RDBMS, *three-tier web application* dan lain- lain.

Tanggung Jawab

Tanggung jawab IT adalah untuk memastikan bahwa semua *software* yang ter-*install* dan operasional dalam lingkungan Danareksa dilingkupi dengan lisensi *software* yang mencukupi dan *up-to-date*, sesuai dengan kebutuhan dan kemampuan Danareksa.

Kebijakan

a. IT akan membuat suatu standar *software* yang akan direkomendasikan untuk di-*install* pada setiap komputer pegawai dan digunakan dalam tugas operasionalnya sehari-hari. *Software* standar tersebut telah dianggap dapat memenuhi kebutuhan operasional Danareksa sehari-hari. Penggunaan *software* standar ini akan diatur Danareksa dari segi lisensi-nya.
b. Disamping *software* standar di atas, pegawai yang mempunyai kebutuhan *software* khusus lainnya dapat mengajukan permintaan ke Direksi terkait dengan sepengetahuan dan persetujuan IT. Pengurusan lisensi *software* tersebut untuk kasus seperti ini akan dilakukan sendiri oleh pegawai masing-masing, dengan bantuan dari IT.
c. Pihak IT akan tetap menyimpan *software* versi lama, termasuk semua komponen yang diperlukannya untuk operasional, jika diperlukan dalam rangka *restore* data lama dari media *tape backup*.
d. Pegawai tidak diperbolehkan untuk melakukan *install software* lainnya tanpa sepengetahuan IT. Jika hal ini terjadi, maka segala konsekuensi yang diakibatkan oleh *software* tersebut, misalnya komputer *crash* atau terserang virus, sepenuhnya menjadi tanggung jawab pegawai yang bersangkutan.
e. Penggunaan *software* yang tidak mempunyai lisensi akan menjadi tanggung jawab masing-masing pengguna dimana Danareksa dibebaskan dari segala tuntutan dan tanggung jawab mengenai penggunaan *software* ilegal tersebut.
f. Danareksa akan melakukan audit internal secara berkala terhadap penggunaan softwarenya.
g. Pegawai dilarang secara melawan hukum memiliki, menggunakan, dan menyebarkan *software* ataupun barang-barang yang dilindungi oleh hak cipta lainnya seperti game, MP3, CD musik, ataupun media lainnya di dalam lingkungan Danareksa.

h. Segala pelanggaran terhadap kebijakan dan peraturan ini dapat dikenakan sanksi seperti yang diatur pada Kebijakan Penanganan Insiden dan Sanksi, dari tindakan disipliner ringan sampai kepada tindakan pemberhentian yang bersangkutan.

IX.10. Penggunaan Perangkat Komputer

Tujuan

Untuk memastikan bahwa perangkat komputer Danareksa yang disediakan untuk para pegawai digunakan dengan semestinya, untuk tujuan operasional Danareksa, dan juga sesuai dengan aturan perundangan yang berlaku.

Ruang Lingkup

Kebijakan ini mencakup penggunaan perangkat komputer seperti PC, *notebook*, *server*, *Smartphone*, dan perangkat komputer lainnya yang tersambung ke PC atau *notebook* Danareksa. Perangkat tambahan yang dicakup terutama yang dapat berfungsi sebagai alat penyimpan atau pengirim data. Kebijakan pemakaian ini juga mencakup *printer*, *scanner*, *multi-function printer* (*fotocopy* dan *print*), dan peralatan pencetak lain.

Tanggung Jawab

a. Pihak IT wajib menyediakan perangkat komputer yang digunakan untuk mendukung kegiatan kegiatan bisnis dan operasional dengan *software* standar termasuk *operating system*-nya, serta mengatasi segala gangguan operasional yang terjadi atas perangkat tersebut.
b. Semua pegawai wajib ikut menjaga keamanan informasi dan perangkat komputer yang sehari-hari dipakainya, baik di dalam maupun di luar lingkungan Danareksa.

Kebijakan

a. Seluruh perangkat komputer yang disediakan untuk pada pegawai Danareksa dalam operasionalnya sehari-hari harus digunakan untuk kepentingan Danareksa. Pegawai dilarang untuk menggunakan perangkat komputer tersebut untuk hal-hal yang berhubungan dengan bisnis pribadi maupun kepentingan non-bisnis lainnya.
b. Setiap pengguna komputer tidak diperkenankan melakukan modifikasi atau penambahan peralatan pribadi yang dapat mempengaruhi kinerja komputer Danareksa, kecuali sudah mendapatkan persetujuan dari IT dan dilakukan dengan sepengetahuan IT.

c. Setiap pegawai bertanggung jawab atas keamanan, kebersihan, dan kondisi komputer kerjanya. Apabila ditemukan kerusakan yang dilakukan dengan unsur kesengajaan maka perbaikan yang terjadi akan dibebankan kepada staf yang bersangkutan.
d. Untuk pegawai yang menggunakan *notebook* atau *portable computer* lainnya, maka unsur keamanan yang menjadi tanggung jawab pegawai termasuk dari risiko kehilangan dan pencurian. *Notebook* yang dibawa keluar kantor harus menggunakan koper/tas *notebook* dan tidak boleh ditinggalkan tanpa pengawasan di tempat umum.
e. Khusus untuk pengguna *computer portable* ini, maka harus dilakukan tambahan pengamanan terhadap data yang tersimpan dalam komputer tersebut, yang detailnya akan diberikan oleh IT. Jika pengamanan ini tidak dapat dilakukan pada komputer portable tersebut, maka komputer tersebut tidak boleh memuat data yang sifatnya sensitif.
f. Pengguna komputer harus mematikan komputernya dengan sempurna (*shut down*) apabila hendak meninggalkan kantor.
g. Pegawai Danareksa tidak boleh mengakses komputer selain dari yang digunakannya sehari-hari, tanpa ijin pemilik komputer tersebut. Jika ada pengalihan hak atas penggunaan komputer, maka ini harus dilakukan oleh dan sepengetahuan IT, yang telah berkoordinasi dengan unit kerja pegawai yang lama maupun yang baru.
h. Penggunaan *removable storage* dinonaktifkan, Staf yang mempunyai tugas khusus dapat mengajukan izin tertulis dari Kepala Divisi yang bersangkutan untuk menggunakan *removable storage*.
i. Setiap pegawai harus menggunakan printer secara efektif dan efisien, dengan menggunakan *shared printer* yang ada di sekitarnya. Penggunaan printer secara pribadi diperbolehkan apabila yang bersangkutan sering terkait dengan hal-hal yang bersifat rahasia. Instalasi printer pribadi ini harus mendapatkan persetujuan Direksi.

j. Penggunaan perangkat komputer di lingkungan Danareksa harus selalu mengedepankan keamanan informasi sensitif dan keamanan perangkat tersebut. Jika pegawai Danareksa meninggalkan komputernya dalam waktu yang lama, maka komputer tersebut harus dilindungi dari akses orang lain, minimal dengan *password screen saver* atau *lock computer*.
k. Semua perangkat komputer harus dipastikan menggunakan pelindung dari lonjakan arus (*power strip*) atau UPS (baterai cadangan).
l. IT dimungkinkan untuk melakukan pemeriksaan secara berkala atau sewaktu-waktu, terhadap kondisi dan pemakaian perangkat komputer.

m. Jika staf yang mendapatkan alokasi perangkat komputer tidak lagi bekerja pada Danareksa, berdasarkan konfirmasi dari HC, maka perangkat tersebut harus dikembalikan ke IT efektif pada hari terakhir staf yang bersangkutan bekerja dan berada di kantor Danareksa. IT harus memastikan bahwa staf atau Divisi yang bersangkutan sudah tidak lagi memiliki akses perangkat tersebut. Hal ini dapat dimasukkan sebagai bagian dari *exit procedure* yang berlaku di Danareksa.
n. Segala pelanggaran terhadap kebijakan dan peraturan ini dapat dikenakan sanksi seperti yang diatur pada Kebijakan Penanganan Insiden dan Sanksi, dari tindakan disipliner ringan sampai kepada tindakan pemberhentian yang bersangkutan.

IX.11. Penggunaan Internet

Tujuan

Untuk memastikan bahwa perangkat komputer Danareksa yang disediakan untuk para pegawai digunakan dengan semestinya, tersambung dengan internet, untuk tujuan operasional Danareksa, dan juga sesuai dengan aturan perundangan yang berlaku.

Ruang Lingkup

Kebijakan ini mencakup penggunaan perangkat komputer seperti PC, *notebook*, *server*, *Smartphone*, dan perangkat komputer lainnya yang tersambung ke PC atau *notebook* Danareksa. Perangkat tambahan yang dicakup terutama yang dapat berfungsi sebagai alat penyimpan atau pengirim data. Kebijakan pemakaian ini juga mencakup *printer*, *scanner*, *multi-function printer* (*fotocopy* dan *print*), dan peralatan pencetak lain.

Tanggung Jawab

a. Divisi IT wajib memastikan bahwa perangkat komputer Danareksa tersambung dengan internet.
b. Semua pegawai memanfaatkan koneksi internet untuk mendukung tugas dan pekerjaan.
c. Semua pegawai wajib menjaga keamanan dari ancaman melalui internet.

Kebijakan

a. Fasilitas Internet diadakan untuk menunjang pekerjaan pegawai Danareksa sesuai dengan kepentingan/tujuan Danareksa. Danareksa mempunyai wewenang untuk melakukan pembatasan cara, waktu atau kapasitas akses ke situs-situs Internet tertentu dengan menggunakan *Internet Proxy* atau jalur khusus, dipandang dari kepangkatan, unit kerja, dan kebutuhan pegawai dalam menunjang pekerjaannya.

b. Semua penggunaan internet melalui jaringan Danareksa akan dipantau dan dicatat secara formal meliputi *User* ID, sumber IP, tanggal, waktu, protokol, dan situs tujuan atau *server* dan dapat diperiksa dalam rangka kegiatan monitoring atau audit keamanan informasi.
c. Akses ke Internet oleh pegawai harus menggunakan fasilitas yang telah disediakan oleh Danareksa, dari *software browser* yang digunakan, jalur akses ke Internet untuk akses pegawai, dan lain-lain yang intinya untuk meminimalkan risiko dan ancaman virus, *active script*, *spyware*, dan lain-lain yang dapat membahayakan layanan dan operasional Danareksa.
d. Setiap pegawai bertanggung jawab atas semua kegiatan yang berkaitan dengan Internet, yang dilakukan dengan menggunakan otorisasi *username* dan *pasword* ke jaringan internet Danareksa.
e. Penggunaan Internet untuk keperluan pribadi merupakan hal yang tak terhindarkan, dan dapat ditolerir oleh Danareksa sepanjang tidak mengganggu pekerjaan utama yang bersangkutan, yang akan diputuskan oleh manager yang bersangkutan.
f. Pegawai dilarang menggunakan jejaring media sosial tentang Danareksa.
g. Karena keterbatasan akses ke Internet, pegawai dilarang untuk melakukan kegiatan yang membutuhkan *bandwidth* besar selama jam kerja Danareksa.
h. Internet tidak boleh dipergunakan untuk mengungkap informasi Danareksa bila tidak berwenang dan kegiatan yang menyinggung orang lain atau yang berhubungan dengan SARA, politik, fitnah, pornografi, perjudian dan lain-lain. Internet tidak boleh dipergunakan untuk kegiatan yang melanggar peraturan perundangan yang berlaku, terutama yang menyangkut hak atas kekayaan intelektual, seperti kegiatan *download streaming video*, musik dan lainnya.
i. Pegawai tidak boleh menggunakan layanan Internet Danareksa untuk alasan komersial lainnya yang berhubungan dengan keuntungan finansial pribadi, misalnya melalui media sosial, *online store*, *online gambling*, permainan dan lain-lain.
j. Bila pegawai ingin mengakses situs yang diblokir karena sesuai dan diperlukan untuk tujuan bisnis maka pegawai harus mengajukan permohonan pengecualian akses secara tertulis kepada Kepala Divisi yang bersangkutan. IT akan mengevaluasi penggunaan *site* un-blokir tersebut sesuai dengan pemanfaatannya.
k. Untuk keperluan layanan transaksi nasabah melalui Internet harus disediakan jalur komunikasi khusus dari perusahaan penyedia layanan Internet, yang terpisah dari layanan Internet data untuk pegawai Danareksa.
l. Danareksa akan menjaga kinerja, keamanan dan citra yang ditampilkan untuk layanan terhadap nasabah Danareksa melalui jalur internet.

m. Danareksa harus menggunakan peralatan, *software* ataupun layanan tambahan untuk mengamankan dan memonitor penggunaan jalur Internet ini.
n. Danareksa harus melakukan suatu IT *security* audit yang mencakup layanan Internet Danareksa yang akan diatur dan dilakukan oleh Divisi Internal Audit.
o. Setiap insiden yang berhubungan dengan keamanan atas fasilitas Internet dan *server* yang dihubungkan langsung ke Internet harus segera ditindak lanjuti oleh *Information Security Officer* (ISO) dan dilakukan *logging* secara rinci untuk kepentingan pencatatan dan pengusutan dan hal lain yang diperlukan. Pelaporan atas insiden ini akan diberikan secara lengkap oleh ISO kepada IT dan Direksi. Direksi dapat meminta IT untuk melakukan investigasi lebih lanjut, membuat rencana eskalasi dan perbaikan yang diperlukan.
p. Segala pelanggaran terhadap kebijakan dan peraturan ini dapat dikenakan sanksi seperti yang diatur pada Kebijakan Penanganan Insiden dan Sanksi, dari tindakan disipliner ringan sampai kepada tindakan pemberhentian yang bersangkutan.

IX.12. Klasifikasi Informasi

Tujuan

Dengan membagi informasi berdasarkan beberapa klasifikasi yang berkaitan dengan kepentingan Danareksa, maka didapatkan cara penanganan informasi yang lebih efisien dan praktis.

Ruang Lingkup

Seluruh informasi operasional Danareksa.

Tanggung Jawab

a. Seluruh pemilik informasi bertanggung jawab atas klasifikasi dan perlindungan terhadap informasi yang dimilikinya, apapun medianya.
b. IT bertanggung jawab dalam menyediakan suatu sistem kontrol akses pada media penyimpanan informasi yang bersifat elektronik. Untuk sistem kontrol akses terhadap media penyimpan di luar IT, IT akan membantu, mengkoordinasikan dan menyetujui sistem yang diimplementasikan.

Klasifikasi Informasi

Berdasarkan tingkat kerahasiaannya, informasi dapat diklasifikasikan sebagai berikut:

a. **Sangat Rahasia/*Top Secret***:
   Hanya diketahui oleh pihak-pihak yang sangat terbatas yang diberi akses langsung oleh pemilik informasi dan tidak dapat diberitahukan kepada pihak lain.

b. **Rahasia/*Confidential***:
Hanya diketahui oleh pihak-pihak yang memenuhi kriteria tertentu sesuai yang ditetapkan oleh pemilik informasi.
c. **Terbatas/*Restricted***:
Hanya ditujukan untuk pihak-pihak tertentu, namun ada kemungkinan dapat diakses oleh pihak-pihak lain yang tidak dimaksudkan untuk menerima informasi tersebut.

d. **Umum/*Public***:
Informasi yang bisa diakses oleh siapapun.

Dasar dari pengklasifikasian diatas dapat berasal dari:
a. Klasifikasi yang ditentukan oleh negara atau pemerintah;
b. Kesepakatan dalam perjanjian;
c. Regulasi yang berlaku;
d. Peraturan perusahaan;
e. Pertimbangan “privacy”; dan
f. Pertimbangan keamananan.

Dampak dari memperlakukan informasi tidak sesuai dengan klasifikasinya antara lain:
a. Tuntutan pidana;
b. Tuntutan perdata;
c. Denda;
d. Melemahkan persaingan; dan
e. Dicabut atau dilakukan *suspend* terhadap ijin yang dimiliki institusi atau perorangan yang melanggar klasifikasi tersebut.

Klasifikasi informasi digunakan untuk menerapkan pengamanan jenis apa yang relevan terhadap informasi yang telah diklasifikasi. Tidak semua informasi akan mendapatkan perlakuan dan perlindungan yang sama.

Perlakuan dan perlindungan terhadap informasi yang telah diklasifikasikan lebih diutamakan dalam hal penyimpanan dan pengiriman informasi tersebut. Perlakuan ini tidak membedakan media atau bentuk informasi yang ada.

Perubahan klasifikasi informasi dapat terjadi, misalnya, antara lain karena perubahan kepentingan dari informasi rahasia menjadi informasi publik, informasi yang lewat waktu atau kadaluarsa, regulasi dan sebagainya.

Selain dari klasifikasi informasi, setiap informasi yang berkaitan dengan operasional Danareksa akan diidentifikasikan pemiliknya. Pemilik informasi adalah mereka yang

secara langsung mempunyai akses ke informasi termaksud, dan tidak berarti hanya originator dari informasi termaksud.

Kebijakan

a. Pemilik informasi harus menentukan klasifikasi pertama atas informasi berdasarkan kriteria di atas, kemudian penerima informasi harus memperlakukan informasi tersebut sesuai dengan klasifikasi yang telah diberikan. Jika salah satu pemilik merubah klasifikasi informasi tersebut, maka perubahan ini harus diberitahukan kepada semua penerima informasi lainnya. Jika perubahan klasifikasi ini menyangkut versi baru dari informasi tersebut, maka hanya informasi dengan versi yang sama atau lebih baru yang berubah klasifikasinya. Sejak saat tersebut, perlakuan dan perlindungan terhadap informasi ini diperlakukan dengan mengacu kepada klasifikasi yang baru.
b. Jika beberapa informasi disimpan secara bersama-sama, maka kelompok informasi tersebut mendapatkan klasifikasi sesuai dengan klasifikasi tertinggi dari informasi yang ada dalam kelompok informasi tersebut. Contoh: jika satu unit informasi Rahasia disimpan bersama dengan satu unit informasi Umum, maka kelompok dua unit informasi ini mempunyai klasifikasi Rahasia.
c. Informasi dengan klasifikasi rahasia ke atas harus disimpan pada suatu sistem yang dilengkapi dengan suatu kontrol akses, misalnya *file server*, *maildrop*, atau lemari terkunci untuk yang berwujud *hardcopy*. Pemilik informasi harus berkoordinasi dengan IT untuk menerapkan kontrol akses terhadap informasi elektronik yang dimilikinya, sesuai dengan ketentuan yang berlaku. Penyimpanan file dengan klasifikasi di atas pada media penyimpanan seperti CD, *flash disk*, *memory card*, dan sebagainya, hanya diperbolehkan jika ditambahkan dengan kontrol akses seperti *encryption* ataupun *password* akses. Tatacara pemberian kontrol akses ini harus diketahui dan disetujui oleh IT, berkenaan dengan kebijakan kontrol akses terhadap informasi yang telah diatur terpisah.
d. Penyimpanan file elektronik pada komputer lokal, jika memiliki klasifikasi rahasia ke atas, harus ditambahkan kontrol akses seperti *encryption* atau *password*. Tatacara pemberian kontrol akses ini harus diketahui dan disetujui oleh IT, berkenaan dengan kebijakan kontrol akses terhadap informasi yang telah diatur terpisah.
e. Transmisi file elektronik dengan klasifikasi Rahasia ke atas harus dengan sistem *encryption* yang memastikan benar-benar diterima oleh pihak yang dituju. Transmisi file elektronik dengan klasifikasi Khusus harus memperhatikan bahwa penerima adalah benar-benar mereka yang dituju.
f. Pengiriman informasi *hardcopy* dengan klasifikasi Rahasia ke atas harus dengan jasa kurir yang telah dipercaya dan telah mengikuti segala kebijakan keamanan informasi

Danareksa. Pengiriman informasi *hardcopy* dengan klasifikasi Khusus harus dengan metode yang tercatat.

g. Pencetakan informasi dengan klasifikasi Rahasia ke atas harus dengan perangkat yang terpisah dan dapat dibatasi aksesnya secara fisik. Pencetakan informasi dengan klasifikasi Khusus dapat dilakukan pada perangkat umum dengan batasan bahwa akses terhadap informasi tersebut dapat dijaga.
h. Segala pelanggaran terhadap kebijakan dan peraturan ini dapat dikenakan sanksi seperti yang diatur pada Kebijakan Penanganan Insiden dan Sanksi, dari tindakan disipliner ringan sampai kepada tindakan pemberhentian yang bersangkutan.

IX.13. Kontrol terhadap Akses Data

Tujuan

Untuk memastikan bahwa akses terhadap informasi Danareksa hanya diberikan kepada dan dilakukan oleh pihak-pihak yang berhak dan telah mendapatkan akses tersebut sesuai dengan prosedur yang berlaku. Hal ini juga berlaku untuk meningkatkan keamanan akses terhadap informasi yang disediakan oleh Danareksa.

Ruang Lingkup

Untuk memastikan bahwa akses terhadap informasi Danareksa hanya diberikan kepada dan dilakukan oleh mereka yang berhak dan telah mendapatkan akses tersebut sesuai dengan prosedur yang berlaku.

Tanggung Jawab

a. IT bertanggung jawab untuk menjaga tingkatan akses dari sisi *server* yang digunakan Danareksa. Seluruh pemilik informasi bertanggung jawab atas klasifikasi dan perlindungan terhadap informasi yang dimilikinya, apapun medianya.
b. Setiap pegawai Danareksa wajib mengetahui setiap risiko dan konsekuensi tindakan yang dilakukannya dalam rangka keamanan informasi ini.

Kebijakan

a. Standar akses terhadap informasi/sistem aplikasi diatur dan disesuaikan dengan kebutuhan bisnis pada tingkatan kelompok atau unit kerja, secara konsisten pada seluruh Danareksa, dengan tetap memperhatikan keamanan informasi/sistem yang akan di akses. Akses tersebut akan dikontrol secara ketat untuk menghindarkan akses dari orang-orang yang tidak berhak.

b. Pada setiap sarana penyimpan informasi ini, Danareksa harus melakukan pencatatan akses (*audit trail*) sebagai bahan pemeriksaan konsistensi akses dan konsistensi data tersebut, serta untuk deteksi dan investigasi insiden akses. Pencatatan dilakukan paling tidak untuk semua akses (*object access*), baik yang berhasil maupun yang gagal (*success and failure*), yang akan dijaga selama satu bulan penuh, dan termasuk dalam data yang akan masuk dalam *backup* bulanan. Setelah dilakukan *backup* bulanan, maka data *audit trail* yang ada dapat di-*overwrite* dengan data yang baru.
c. Audit trail tersebut akan menjadi dasar bagi suatu *security audit* yang akan dilakukan oleh Divisi Internal Audit.
d. Pegawai yang memiliki akses ke informasi tertentu dilarang untuk melakukan modifikasi akses atau melakukan delegasi akses kepada pegawai lain, dan dilarang memberikan informasi dengan akses terbatas tersebut kepada mereka yang tidak berhak.
e. Pegawai yang merupakan administrator atau kustodian dari data atau kelompok data seperti *database* aplikasi, wajib menjaga konsistensi akses dan konsistensi data yang ada dalam kuasa administratifnya, termasuk memastikan bahwa masing-masing *User* menjaga dan menggunakan aksesnya secara semestinya.
f. Pegawai tidak diperbolehkan melakukan *full share* (*read dan write permission* – seperti “Everybody” “Full Control”) pada *harddisk* atau komputer.
g. Pegawai dilarang untuk menggunakan informasi Danareksa yang dapat diaksesnya untuk kepentingan pribadi berupa keuntungan finansial pribadi secara langsung, ataupun kepentingan lain yang bertentangan dengan kebijakan keamanan informasi lainnya.
h. Segala surat menyurat ataupun tempat transit media informasi harus terlindung dari pihak-pihak yang tidak berhak/berkepentingan.
i. Hasil cetak informasi dengan akses terbatas harus dijaga oleh yang bersangkutan agar tidak terbuka akses ke pihak-pihak yang tidak berhak.
j. Selanjutnya akses terhadap media cetak berisikan informasi terbatas tersebut harus tetap terlindung, khususnya di luar jam kerja atau di saat pemilik informasi tidak berada di tempatnya.
k. Semua Informasi elektronik yang tersimpan dalam perangkat *server*, komputer kerja, komputer penghubung, laptop, *smartphone* atau *mobile device* lainnya, bila tidak dipergunakan tidak boleh ditinggalkan dalam keadaan *logged on* tanpa pengawasan, harus dilindungi menggunakan kunci pin, *password* atau alat kontrol lain yang secara periodik dirubah.
l. Setiap informasi yang bersifat transaksional dan data nasabah harus dilakukan enkripsi sebelum dikirimkan melalui jaringan komputer dari pengirim maupun

penerima. Metode enkripsi yang dipilih akan dijabarkan lebih lanjut pada prosedur operasional mengenai kontrol terhadap akses data.

m. Informasi yang bukan bersifat umum/biasa tidak boleh dikirimkan melalui transmisi umum dan hanya dapat dikirimkan dan diterima oleh dengan metode pengiriman yang aman, apabila hal tersebut tidak dapat dilakukan maka pengirim dan penerima harus dipastikan dilakukan oleh orang yang berwenang.
n. Data yang akan dikirim/diberikan kepada pihak lain termasuk pihak ketiga, yang berkenaan dengan proses operasional Danareksa maupun berkenaan dengan peraturan perundangan yang berlaku, seperti misalnya laporan kepada badan regulator, harus dilakukan dengan mengacu pada kebijakan ini.
o. Mesin pengganda dokumen seperti mesin foto kopi, mesin fax, atau CD-ROM *writer* harus terkunci atau dilindungi dari penggunaan oleh pihak tak berwenang di luar jam kerja normal.
p. Segala pelanggaran terhadap kebijakan dan peraturan ini dapat dikenakan sanksi seperti yang diatur pada Kebijakan Penanganan Insiden dan Sanksi, dari tindakan disipliner ringan sampai kepada tindakan pemberhentian yang bersangkutan.

IX.14. Retensi dan *Backup Data*

Tujuan

Untuk memastikan bahwa penyimpanan data sesuai dengan tujuan untuk mendukung operasional.

Ruang Lingkup

Kebijakan ini mencakup seluruh media penyimpan data dengan proses penyimpanan, *restore*, dan penghancuran masing-masing media. Tujuannya adalah supaya informasi perusahaan dapat diakses oleh mereka yang berhak saat diperlukan.

Tanggung Jawab

a. Tanggung jawab setiap pemilik data adalah melakukan klasifikasi data yang dimilikinya, dan memberikan masa retensi pada data tersebut, serta memastikan bahwa semua datanya telah di-*backup* sesuai dengan ketentuan dan kebutuhan.
b. Tanggung jawab IT untuk memastikan bahwa data yang tersimpan dalam *file server* dapat diakses secara handal, dimana diperlukan oleh pemilik dan pemakainya.
c. Tanggung jawab IT adalah untuk melakukan penyimpanan data sesuai dengan klasifikasi dan retensi di atas, melalui suatu sistem *backup*, *restore*, dan *offsite storage* secara efektif dan efisien.

Kebijakan

a. Untuk setiap data tersimpan, harus dilakukan kebijakan retensi masing-masing, yang akan digunakan sebagai pedoman IT untuk memastikan tingkat reliabilitas data termaksud. Hal ini akan disesuaikan dengan ketentuan Danareksa maupun peraturan perundangan yang berlaku.
b. Berdasarkan klasifikasi atas informasi yang diberikan, maka harus dilakukan pembedaan sistem akses dan *backup* yang dipilih, yang nantinya akan membuat data yang sangat dibutuhkan oleh operasional Danareksa mendapat perhatian semestinya dan dapat diakses secara kontinyu.
c. Suatu sistem *backup* harus dipilih untuk semua informasi yang disimpan di *file server*, dimana aplikasinya harus sesuai dengan huruf (a) di atas.
d. Penyimpanan media *backup* harus mengikuti Kebijakan yang berlaku, untuk peletakan media *backup* di lokasi *off site*.
e. Jika data yang harus di-*restore* berada pada lokasi *off site*, maka kecepatan pengambilan kembali dan proses *restore* yang diperlukan harus dapat diterima oleh para pemilik data.
f. Tempat penyimpanan media *backup* harus disesuaikan dengan persyaratan yang ada, untuk meminimalkan risiko kegagalan *restore* karena media yang rusak. Persyaratan yang sama harus dipenuhi oleh lokasi *off site* yang dipilih.
g. Semua proses *backup* harus dicatat dengan lengkap dan *reliable*, untuk mempermudah proses *restore* data tersebut dimana diperlukan. Semakin tinggi kebutuhan akan data maka semakin cepat proses *restore* dilakukan. Kemungkinan media *backup* tidak terlacak harus ditekan sekecil mungkin.
h. Dilakukan *test* secara periodik atas media *backup* yang ada, untuk memastikan bahwa data pada media tersebut dapat di-*restore* dengan baik. Setiap *test* yang dilakukan akan dicatat secara formal.
i. Jika masa retensi data atau informasi sudah lewat, maka IT dapat langsung melakukan rotasi media *backup* yang termaksud, kecuali ada permintaan khusus dari pemilik data untuk memperpanjang masa retensi.
j. Jika data berwujud pada media yang tidak dapat dipakai kembali, maka IT dapat langsung menghancurkan data yang sudah lewat dari masa retensinya. Proses penghancuran ini akan dilakukan secara tercatat dan dengan dihadiri oleh saksi eksternal IT.

IX.15. Keamanan Informasi di Lingkungan Kerja

Tujuan

Untuk memastikan keamanan informasi di lingkungan kerja pegawai Danareksa.

Ruang Lingkup

Seluruh pegawai Danareksa dan seluruh informasi di lingkungan kerja, termasuk di lokasi penyimpanan dokumen yang bersifat *offisite*.

Tanggung Jawab

Seluruh pegawai, terutama para pemilik informasi yang sifatnya terbatas harus sadar akan risiko dan konsekuensi tindakannya atas informasi yang dimilikinya.

Kebijakan

a. Komputer kerja dan komputer penghubung tidak boleh ditinggalkan dalam keadaan *logged on* tanpa pengawasan, serta harus dilindungi dengan menggunakan kunci, *password* dan alat kontrol lain seperti *screen saver*, bila tidak sedang dipergunakan. IT harus memastikan bahwa konfigurasi komputer standar untuk pegawai sudah di-*set up* untuk hal keamanan dan keselamatan informasi.
b. Seluruh pegawai harus menyimpan seluruh dokumen yang berkaitan dengan Danareksa dan bersifat **Rahasia** apabila menerima tamu di meja kerjanya.
c. Seluruh pegawai harus menyimpan seluruh dokumen dalam bentuk *hardcopy* atau elektronik yang berkaitan dengan Danareksa, terutama yang bersifat **Rahasia** di tempat yang terkunci apabila hendak meninggalkan kantor.
d. Jika dilakukan *routing* internal, pengiriman ataupun penggandaan dokumen, terutama dengan klasifikasi **Rahasia**, maka harus dipastikan bahwa akses terhadap dokumen ini selama *routing*, pengiriman ataupun penggandaan dilakukan tetap terjaga pada mereka yang berhak.
e. Seluruh pegawai harus menghapus atau menghilangkan seluruh tulisan atau bahan yang berada di papan tulis atau di meja ruang meeting apabila telah selesai melakukan *meeting*/pertemuan.
f. Semua printer dan mesin fax harus dibersihkan dari kertas segera setelah mencetak dan memastikan bahwa dokumen sensitif tidak tersisa di printer yang dapat diakses orang lain yang tidak berhak.
g. Seluruh pegawai harus memastikan bahwa informasi yang tersedia di lingkungan kerjanya tidak dapat dipergunakan secara tidak semestinya oleh orang lain. Hal ini dapat juga disebut ”clean desk clean screen policy”.
h. Seluruh pegawai tidak diperbolehkan memberikan akses dengan cara apapun terhadap informasi yang disediakan Danareksa kepada orang lain yang tidak berhak, baik secara sengaja ataupun tidak disengaja. seperti teknik rekayasa sosial (*social engineering*) mengaku sebagai reporter, konsultan, kontraktor, pihak terafiliasi atau lainnya melalui telepon, e-mail, media sosial, pesan pribadi atau komunikasi lain. Jika identitas pihak tersebut tidak bisa diverifikasi, pegawai harus segera menghubungi atasan/manajer langsung.

i. Segala pelanggaran terhadap kebijakan dan peraturan ini dapat dikenakan sanksi seperti yang diatur pada Kebijakan Penanganan Insiden dan Sanksi, dari tindakan disipliner ringan sampai kepada tindakan pemberhentian yang bersangkutan.

IX.16. Audit Keamanan Informasi

Tujuan

Untuk memastikan bahwa kebijakan dan prosedur keamanan informasi yang telah ditetapkan Danareksa secara aktif dilakukan oleh semua pegawai Danareksa, dan pihak lainnya yang terkait.

Ruang Lingkup

Audit terhadap seluruh peraturan, proses dan prosedur keamanan informasi di lingkungan Danareksa.

Tanggung Jawab

a. Seluruh pemilik informasi wajib memastikan bahwa kebijakan audit ini dilakukan untuk informasi yang berada dalam kontrolnya.
b. Pihak internal audit dan IT akan secara berkala melakukan audit keamanan informasi.

Kebijakan

a. Keamanan informasi merupakan suatu faktor yang penting bagi operasional Danareksa, dan oleh karenanya audit terhadap keamanan informasi secara rutin ataupun karena keperluan tindak lanjut investigasi insiden harus dilakukan oleh Danareksa. Pihak Internal Audit akan merencanakan audit informasi yang jadwal dan lingkupnya akan ditentukan oleh Internal Audit dan akan menetapkan keperluan pihak-pihak lain seperti IT ataupun pihak eksternal untuk membantu dalam melakukan audit. Dalam hal diperlukan pihak eksternal, maka akan dilakukan koordinasi dengan Direksi atau Kepala Divisi.
b. Kegiatan audit akan didasarkan pada seluruh kebijakan, proses, dan prosedur yang berlaku dan yang berkaitan dengan keamanan informasi. Untuk kegiatan audit internal ini akan disiapkan suatu *template* dan *checklist* audit yang akan menjadi dasar kerja proses audit yang terjadi.
c. Semua pihak yang telah menyetujui jadwal di atas wajib membantu kelancaran kerja tim audit internal maupun eksternal.
d. Pihak auditor akan memberikan laporan akhir audit yang dilakukannya kepada IT yang kemudian menyebarkannya kepada semua pihak terkait. Dalam prosesnya

diberikan jangka waktu dimana semua pihak terkait dapat melakukan klarifikasi atau jawaban terhadap laporan yang dibuat. Pada akhir jangka waktu tersebut, semua jawaban dan klarifikasi yang diterima akan dicakup dalam appendix laporan audit final yang dibuat.

IX.17. Akses Pihak Ketiga

Tujuan

Untuk memastikan bahwa akses terhadap layanan informasi atau transaksi yang disediakan Danareksa hanya digunakan oleh pihak ketiga yang berhak dan telah mendapatkan akses tersebut sesuai dengan prosedur yang berlaku. Hal ini juga berlaku sebaliknya dimana Danareksa menggunakan akses dan fasilitas yang disediakan oleh pihak ketiga lain.

Ruang Lingkup

Kebijakan ini mencakup semua sambungan ke jaringan Danareksa, baik yang dilakukan secara perorangan atau perusahaan pihak ketiga, sesuai dengan kontrak kerja yang telah disepakati, dan untuk tujuan serta jenis akses yang telah disepakati.

Akses pihak ketiga didefinisikan sebagai akses pada informasi dengan klasifikasi Rahasia ke atas, dengan menggunakan jaringan Danareksa, dan oleh pihak-pihak di luar Danareksa seperti konsultan, auditor, tamu serta pemasok, dalam kerjasamanya dengan pihak Danareksa. Akses ini dapat berupa akses sementara oleh personil yang ditunjuk ke dalam jaringan Danareksa (akses jenis P = personal), atau akses yang bersifat permanen dalam kaitan kerjasama operasional antara kedua Danareksa (akses jenis B = bisnis). Di lain pihak, akses pihak ketiga juga mencakup akses yang diperlukan oleh Danareksa terhadap jaringan ataupun layanan informasi pihak lainnya.

Untuk sambungan jenis P biasanya akan dilakukan di dalam lingkungan Danareksa, atau dengan menggunakan fasilitas dan perangkat Danareksa. Sambungan jenis B biasanya menggunakan metode penyambungan antara kedua jaringan seperti yang disepakati oleh kedua belah pihak.

Tanggung Jawab

a. IT bertanggung jawab untuk menjaga kinerja, ketersediaan dan keamanan sambungan yang telah diberikan kepada pihak ketiga, dan menjaga risiko ke tingkat minimal terhadap akses yang mereka lakukan.

b. Pihak internal Danareksa yang meminta untuk tersambung dengan pihak ketiga wajib memastikan bahwa sambungan yang dilakukan akan memberikan manfaat kepada Danareksa, dan merupakan cara yang paling optimal serta efektif untuk tujuan operasional Danareksa. Mereka wajib melakukan pengawasan bahwa akses pihak ketiga ini digunakan untuk tujuan dan maksud yang telah disetujui bersama.

Kebijakan

a. Pihak internal Danareksa dapat mengajukan permohonan bagi akses pihak ketiga ini kepada Direksi atau Kepala Divisi IT. Setelah mendapatkan persetujuan, pihak IT akan melakukan pemeriksaan, persiapan, dan penyambungan yang diminta.
b. Persyaratan yang diperlukan untuk mengajukan permohonan akses jenis P adalah sebagai berikut:

   i. *Third party connection request*: permohonan untuk mendapatkan akses dengan mencantumkan jenis dan tujuan akses yang diperlukan, jangka waktu akses, kebutuhan bandwidth, serta perangkat atau fasilitas tambahan yang diperlukan. Pada permintaan ini disebutkan secara jelas pihak-pihak yang akan mendapatkan akses ke jaringan Danareksa.
   ii. *Third party network connection agreement*: yang menyatakan bahwa pihak internal Danareksa yang mengajukan telah mengerti hak dan kewajibannya dalam rangka akses ini, serta pihak ketiga termaksud setuju untuk mentaati segala peraturan dan prosedur yang berlaku di lingkungan Danareksa dalam kaitan akses dan keamanan informasi. Jika ada perangkat milik pihak ketiga yang digunakan, maka atas perangkat tersebut pihak ketiga setuju untuk memberikan akses kepada IT sama seperti akses yang dimiliki oleh IT ke perangkat lain serupa milik Danareksa, termasuk untuk melakukan perubahan konfigurasi yang diperlukan.
   iii. *Non-disclosure agreement:* pihak ketiga setuju bahwa informasi dan hal-hal lain yang diperolehnya selama mendapatkan akses ke jaringan Danareksa tidak akan digunakan untuk kepentingan selain kepentingan Danareksa, dan akan memperlakukan informasi tersebut sesuai dengan peraturan Danareksa yang berlaku.
   iv. *Third party contract*: surat kontrak yang melandasi hubungan saling menguntungkan antara Danareksa dengan pribadi/perorangan yang diajukan aksesnya, atau informasi lain yang menjadi justifikasi akses ke jaringan dan informasi Danareksa.

c. Persyaratan yang diperlukan untuk mengajukan permohonan akses jenis B adalah sebagai berikut:
   i. *Third party connection request:* sama dengan poin b.ii. di atas.
   ii. *Third party network connection agreement:* sambungan jaringan Danareksa dengan jaringan Danareksa lainnya akan melewati suatu perangkat pengaman

yang disyaratkan oleh Danareksa, misalnya *edge router* atau *Firewall*. Jika perusahaan lainnya juga mempunyai persyaratan serupa, maka akan dilakukan diskusi mengenai konfigurasi akhir yang disetujui kedua belah pihak. Danareksa tetap mempunyai hak penuh untuk mengatur dan melakukan monitor terhadap perangkat pengaman ini selama koneksi jaringan dilakukan. Jika dikeluarkan biaya tambahan untuk melakukan koneksi jaringan ini, maka kedua belah pihak akan menyetujui hak dan kewajiban dari segi finansial ini sebelum koneksi dilakukan.

iii. *Documentation and configuration diagram*: informasi mengenai tatacara dan protokol sambungan yang dibutuhkan, serta detail dan lokasi sambungan yang akan dilakukan, harus disediakan oleh kedua belah pihak yang melakukan sambungan.

iv. *Non-disclosure agreement*: sama dengan di atas, ada kemungkinan hal ini dilakukan secara dua arah, dalam arti kedua belah pihak mempunyai template masing-masing. *Statement of exclusivity* : jika sambungan jaringan ini bersifat eksklusif, maka diperlukan suatu pernyataan persetujuan bahwa koneksi dengan jenis dan tujuan yang sama tidak akan dilakukan dengan pihak-pihak lainnya, untuk tujuan yang telah disepakati oleh kedua belah pihak. Juga dapat disebutkan di sini apakah perangkat untuk sambungan yang dilakukan dapat dipakai untuk tujuan lainnya oleh kedua belah pihak. Divisi Legal yang membuat dan melakukan *review* atas *non-disclosure agreement*.

v. *Third party contract*: sama dengan poin b.ii. di atas.

d. IT dan pihak terkait lainnya harus melakukan pemeriksaan atas permintaan ini dan segala kelengkapannya, untuk menentukan bahwa akses yang diminta tidak akan memberikan risiko di luar batas toleransi untuk tetap menjaga kinerja dan keamanan jaringan serta informasi Danareksa. Keputusan dan persetujuan akhir untuk sambungan ini berada pada pihak IT, dan atas sepengetahuan Direksi Penanggungjawab IT dan Direksi yang membawahi Divisi terkait yang mengajukan permintaan.

e. IT akan mempersiapkan sambungan yang diminta, dan melakukan konfigurasi minimum untuk memungkinkan jenis dan tujuan akses yang diminta, dalam arti selain jenis dan tujuan yang diminta, tidak dimungkinkan akses lainnya melalui sambungan yang dimaksud. Tatacara pertukaran data dan protokol sambungan akan didiskusikan dan disetujui oleh kedua belah pihak.

f. Jika ada keraguan atas sambungan yang dilakukan, maka dapat dilakukan periode testing oleh kedua belah pihak sampai kedua belah pihak merasa yakin dengan sambungan yang dilakukan.
g. Setelah sambungan selesai dan aktif, maka akan dilakukan pelaporan bulanan oleh kedua belah pihak mengenai sambungan tersebut, dengan pihak Danareksa diwakili oleh IT. Laporan harus memuat hal-hal yang di luar kebiasaan, dimana akan dilakukan pemeriksaan secara kerjasama oleh kedua belah pihak. Untuk Danareksa, laporan akan diterima oleh Direksi atau kepala divisi IT. Setiap triwulan akan dilakukan kajian mengenai sambungan yang dilakukan untuk menetapkan apakah kinerja dan keamanan jaringan Danareksa dan sambungan ke perusahaan lain ini tetap berada pada tingkatan yang dapat diterima Danareksa. Minimal setahun sekali akan dilakukan audit kinerja dan keamanan informasi oleh Divisi Internal Audit terhadap sambungan ini, yang biasanya akan merupakan lingkup audit kinerja dan keamanan informasi Danareksa secara keseluruhan.
h. Setiap perubahan yang dilakukan oleh salah satu pihak pada sambungan jenis B ini harus dikoordinasikan sebelumnya, terutama untuk perubahan yang memiliki risiko terhadap sambungan jaringan. Kedua belah pihak harus melakukan diskusi dan koordinasi sampai kedua pihak setuju jenis perubahan yang tidak akan mengganggu kinerja dan keamanan sambungan.
i. Danareksa telah melakukan segala upaya untuk memperkecil risiko konsekuensi sambungan ini dengan kemampuan yang dimilikinya, dan wajib dibebaskan dari segala tanggung jawab atas terjadinya kerugian akibat sambungan ini pada pihak lainnya.
j. Pada akhir periode kontrak, kedua belah pihak dapat menyetujui untuk mengakhiri sambungan dengan cara yang memiliki risiko minimal terhadap kinerja dan keamanan jaringan kedua belah pihak. Jika sebelum kontrak berakhir salah satu pihak bermaksud untuk memutuskan sambungan ini, maka pihak IT berlaku sebagai pihak yang akan bertanggung jawab dari sisi teknologi informasi untuk melakukan pemutusan yang telah disetujui kedua belah pihak dengan cara yang memiliki risiko minimal terhadap kinerja dan keamanan jaringan kedua belah pihak.
k. Segala pelanggaran oleh pihak internal Danareksa terhadap kebijakan dan peraturan ini dapat dikenakan sanksi seperti yang diatur pada Kebijakan Penanganan Insiden dan Sanksi, dari tindakan disipliner ringan sampai kepada tindakan pemberhentian yang bersangkutan.
l. Pihak ketiga yang terlibat dalam pelanggaran ini akan mendapatkan peringatan keras dari Danareksa, dengan konsekuensi lain yang diatur dalam kontrak kerja dengan pihak tersebut.

X. INFRASTRUKTUR TEKNOLOGI INFORMASI

X.1. Kebijakan *De-Militarized Zone* (DMZ)/Kawasan Batas

Tujuan:

Membentuk, mengatur, dan mengawasi suatu kawasan DMZ, yang memuat informasi dan perangkat informasi yang memang dapat diakses oleh publik. Dengan membatasi akses publik pada DMZ, Danareksa diharapkan memiliki suatu sistem pengamanan terhadap keseluruhan informasi dan perangkat informasi Danareksa terhadap risiko akses yang tidak seharusnya.

Ruang Lingkup:

Seluruh informasi dan perangkat informasi yang terletak di dalam dan pada batas kawasan DMZ (contoh: *switch, router, firewall, web server*, *database server*, serta *server* lainnya).

Tanggung Jawab:

a. Pihak IT akan melakukan pengawasan dan pemeliharaan kawasan DMZ, dan menjaga agar tidak terjadi akses yang tidak seharusnya, baik pada kawasan DMZ itu, maupun ke jaringan internal Danareksa melalui kawasan tersebut.
b. Pihak pemilik informasi yang ditempatkan di DMZ untuk akses publik akan menjaga dan memelihara kesahihan informasi yang ada dan menjaga terhadap akses yang tidak seharusnya, bersama dengan pihak IT.

Kebijakan:

Kebijakan Konfigurasi Perangkat dan Akses

a. DMZ harus sama sekali terpisah dari jaringan internal Danareksa, dan hanya boleh dihubungkan dengan suatu sistem *firewall* yang mengatur akses dari kedua arah.
b. Secara fisik, lokasi perangkat DMZ harus dipisahkan dari lokasi perangkat jaringan internal Danareksa.
c. Jika huruf (b) di atas tidak dimungkinkan, maka harus terdapat batasan yang jelas secara fisik antar keduanya.
d. Untuk perangkat DMZ ini, diatur suatu sistem kontrol akses yang tersendiri, yang mengacu pada bagian IX.2 perihal Kebijakan Akses Ruang Perangkat Teknologi dan bagian IX.17 perihal Kebijakan Akses Pihak Ketiga. Hal ini dilakukan untuk menghindarkan kesalahan koneksi dan konfigurasi antara perangkat DMZ dan perangkat jaringan internal. Akses ke dalam linigkungan DMZ harus dijaga seminimal mungkin dan sesuai keperluan saja. Semua akses untuk hal-hal diluar keperluan tersebut harus ditutup.

e. Sistem dan *server* aplikasi operasional Danareksa tidak boleh terkoneksi langsung pada sistem atau aplikasi yang berada di DMZ. Jika ada pertukaran data dan informasi antar keduanya maka harus dilakukan secara tidak langsung atau melalui suatu sistem *intermediary*.
f. Semua koneksi Danareksa dengan pihak ketiga, termasuk ke Internet, harus dilakukan dengan melewati DMZ untuk alasan keamanan dan keselamatan, serta segala persyaratan oleh pihak ketiga berkenaan dengan koneksi ini harus dilakukan sesuai dengan kebijakan yang telah ditetapkan ini.
g. Semua Kebijakan mengenai Teknologi Informasi, Keamanan dan Keselamatan Informasi yang berlaku pada jaringan internal Danareksa juga berlaku pada kawasan DMZ.
h. Semua perangkat sistem dan aplikasi yang berada di dalam DMZ harus dikonfigurasikan secara aman, dan memenuhi persyaratan keamanan informasi, serta sudah diverifikasi oleh ISO. Layanan yang secara default diberikan oleh sistem, tetapi tidak diperlukan oleh operasional Danareksa, harus dimatikan. Danareksa menetapkan suatu standar konfigurasi aman untuk setiap sistem dan aplikasi yang berada di dalam DMZ, yang diketahui dan dilaksanakan sebagai bagian operasional oleh pihak IT.
i. Semua catatan, dokumentasi dan diagram konfigurasi dari sistem dan aplikasi di DMZ, harus disimpan secara konsolidasi, termasuk sistem pengalamatan dan translasi yang digunakan. Hal ini untuk memudahkan akses ke catatan sistem dan konfigurasi tersebut oleh ISO, IRT, dan pihak IT terkait yang lainnya, bila diperlukan.
j. Semua *security patch*/*hot fixes* untuk sistem, OS, dan aplikasi yang terdapat di DMZ harus di-install secepat mungkin dan sesuai dengan jadwal pemeliharaan yang ada; jika ada penundaan maka harus disesuaikan dengan toleransi risiko yang telah ditetapkan bersama.
k. Jika ada perubahan atas konfigurasi DMZ, baik secara fisik, jaringan, ataupun firewall rule set yang berlaku, yang diusulkan ataupun akan dilakukan oleh pihak IT, maka perubahan tersebut harus tercatat dan disetujui oleh ISO.
l. Segala penambahan maupun pengurangan perangkat harus dilakukan melalui proses persetujuan oleh pihak IT, pihak IRT termasuk ISO.

Kebijakan Pengawasan dan Pengamanan

a. Pihak IT menunjuk satu pihak penanggung jawab perangkat keras dan lunak yang berada di DMZ. Pihak yang dimaksud adalah pihak yang memberikan layanan profesional dan menjaga DMZ (*security managed services company*).
b. Pihak penanggung jawab DMZ secara terus menerus melakukan pengawasan terhadap operasional perangkat keras dan lunak yang berada di DMZ, terutama perangkat pemberi layanan ke publik dan perangkat firewall. Pihak IT harus segera

bertindak jika terjadi gangguan atas perangkat di atas, sesuai dengan SLS/SLA yang telah diberikan.

c. Pihak penanggung jawab DMZ secara terus menerus melakukan review atas *log* dari perangkat keras dan lunak yang berada di DMZ, untuk memastikan tidak ada akses yang tidak seharusnya terjadi.
d. Jika ada kecurigaan atas akses yang terjadi, maka pihak penanggung jawab DMZ harus membuat suatu laporan insiden keamanan informasi yang akan ditindaklanjuti oleh ISO *(Information Security Officer)* dan IRT *(Incident Response Team).*, yaitu personil dan tim IT (*Unit IT Monitoring & Control*).
e. ISO secara berkala melakukan review atas perangkat keras dan lunak DMZ, dalam rangka membantu penanggung jawab DMZ dalam tugasnya sehari-hari.
f. ISO dan penanggung jawab DMZ bersama-sama melakukan review atas *firewall rule* yang ada.
g. ISO harus menjaga dan bertanggung jawab atas kontrol akses yang berlaku pada DMZ, dan secara reguler melakukan review pada daftar ini. Kontrol akses tersebut harus dibatasi pada akses yang benar-benar perlu saja, baik akses oleh publik dan Internet ataupun akses oleh personel internal Danareksa lainnya dalam rangka pemeliharaan sistem ataupun aplikasi yang ada.
h. Perubahan yang telah disetujui atas daftar akses ke DMZ harus dilakukan secepatnya, maksimal 2 (dua) hari setelah tanggal persetujuan. Untuk penghapusan akses yang sifatnya darurat dimungkinkan dilakukan saat itu juga dan disusulkan persetujuannya.
i. Akses untuk pemeliharaan sistem, aplikasi, dan informasi yang dibutuhkan oleh layanan Danareksa yang ada di dalam DMZ harus dilakukan secara aman, misalkan dengan menggunakan jalur enkripsi seperti SSL, IPSEC, contoh: SSH dan HTTPS.
j. Setiap layanan Danareksa yang berada di DMZ akan ditetapkan penanggung jawabnya masing-masing, yang akan dimasukkan dalam daftar akses DMZ. Para penanggung jawab ini bertugas menjaga kelancaran layanannya, sesuai dengan SLA yang ditanggungnya masing-masing. Para penanggung jawab ini harus dapat dihubungi kapanpun untuk keadaan darurat oleh IRT.
k. Jika keadaan memaksa, misalnya terdapat kekhawatiran bahwa suatu layanan DMZ tidak cukup aman, maka prioritas akan diberikan pada jaminan keamanan dan keselamatan informasi, lebih dari ketersediaan layanan tersebut.
l. Sehubungan dengan huruf k di atas, ISO atau penanggung jawab DMZ berhak untuk menghentikan layanan tersebut sampai didapat jaminan mengenai keamanan layanan tersebut, dan atau keamanan DMZ secara keseluruhan.
m. Untuk setiap insiden informasi yang ditemukan pada DMZ, pihak IRT hams menindaklanjuti dengan tindakan investigasi untuk menyimpulkan apa yang terjadi, dan tindakan pengamanan serta preventif-nya.
n. Secara berkala akan dilakukan audit terhadap semua sistem dan fasilitas DMZ, yang akan dikoordinasikan oleh pihak Internal Audit. Dari hasil audit tersebut dapat dilakukan rekomendasi perubahan atas konfigurasi yang aktif, dimana untuk perubahan tersebut akan dilakukan dengan prosedur yang telah disetujui di atas.

X.2. Koneksi Ekstranet dan VPN (*Virtual Private Network*)

Tujuan

Mengatur dan mengawasi semua koneksi ke jaringan internal Danareksa oleh pihak ketiga termasuk oleh pegawai Danareksa dengan menggunakan komputernya sendiri, serta koneksi ke lokasi Danareksa lainnya melalui fasilitas VPN, kecuali koneksi ke Internet, yang digunakan dalam rangka operasional bisnis perusahaan.

Ruang Lingkup

Seluruh informasi dan perangkat informasi dan teknologi yang digunakan dalam membentuk koneksi di atas, baik untuk koneksi individual ke jaringan Danareksa maupun antar jaringan Danareksa yang menggunakan VPN, tidak termasuk koneksi ke Internet. Kebijakan ini terkait sangat erat dengan bagian IX.17 perihal Kebijakan Akses Pihak Ketiga.

Tanggung Jawab

a. Pihak IT akan melakukan pengawasan dan pemeliharaan koneksi tersebut, dan memastikan kinerjanya sesuai dengan SLA (*Service Level Agreement*) yang telah ditetapkan untuk koneksi tersebut. Jika tidak ada SLA yang ditetapkan, maka pihak IT akan memberlakukan SLS standar dan minimum yang berlaku untuk layanan IT kepada *User* Danareksa.
b. Pihak IT wajib mempersiapkan koneksi sesuai dengan kebutuhan yang telah diinformasikan oleh unit kerja Danareksa, termasuk pada pemutusan koneksi ini jika telah tidak dibutuhkan.
c. Pihak pemohon koneksi dari internal Danareksa wajib memastikan bahwa seluruh prosedur koneksi ini telah memenuhi semua persyaratan yang ditetapkan dalam Kebijakan ini dan Kebijakan Akses Pihak Ketiga. Pihak ini juga wajib untuk memantau kontrak dengan pihak ketiga yang berkenaan dengan koneksi ini, dan memberitahukan ke pihak IT 30 hari sebelumnya, jika koneksi tersebut telah tidak diperlukan lagi.
d. Pihak pelaku koneksi ke jaringan Danareksa melalui semua tipe koneksi di atas wajib menjalankan dan memenuhi semua kebijakan IT Danareksa termasuk kebijakan Keamanan dan Keselamatan, terhadap komputer yang digunakannya untuk koneksi ke Danareksa.

Kebijakan

Kebijakan Ekstranet

a. Pihak internal Danareksa yang membutuhkan akses dan koneksi ke pihak ketiga wajib memberitahukan kepada pihak IT secara formal, dan memenuhi segala persyaratan dan prosedur yang ditetapkan dalam Kebijakan Akses Pihak Ketiga,

termasuk penunjukkan penanggung jawab dan nomor kontak di masing-masing pihak.

b. Pihak IT harus dilibatkan sejak awal dalam persiapan koneksi ini, untuk memastikan bahwa koneksi dan titik sambung yang dipilih adalah yang paling efektif dan aman serta memenuhi standar koneksi jaringan yang dimiliki IT. Jika pihak IT telah memiliki koneksi serupa dengan pihak yang sama, maka sedapat mungkin diusahakan menggunakan koneksi yang telah ada tersebut,
c. Jika, ada titik sambung yang berada di lingkungan, User Danareksa, maka titik sambung tersebut harus diberi warna yang berbeda dengan port dari jenis sambungan lainnya, seperti yang ditetapkan dalam Kebijakan Keamanan dan Keselamatan.
d. Dalam hal suatu jaringan eksternal yang melakukan koneksi ke jaringan internal Danareksa rnelalui jaringan ekstranet ini, maka jaringan eksternal tersebut harus memenuhi dan mematuhi semua kebijakan Danareksa mengenai teknologi dan informasi, serta keamanan dan keselamatan.
e. Implementasi koneksi baru ini harus direncanakan dan dilakukan dengan gangguan seminimum mungkin terhadap sistem dan perangkat yang sedang beroperasi. Jika gangguan tidak dapat dihindari, dan akan mengganggu operasional sistem dan layanan lainnya, maka pemberitahuan harus dilakukan oleh pihak IT paling lambat 5 hari dimuka.
f. Segala pemeliharaan, perubahan, pengawasan terhadap jaringan ini akan dilakukan sesuai dengan persyaratan yang dimaksud dalam Kebijakan Akses Pihak Ketiga.
g. Untuk koneksi ekstranet yang dilakukan berdasarkan kontrak dengan pihak ketiga, maka paling lambat 30 hari sebelum kontrak berakhir penanggung jawab koneksi harus memberitahukan ke pihak IT apakah koneksi akan tetap dipertahankan, atau diputus. Jika koneksi akan diputus, maka setelah pihak IT menerima pemberitahuan formal tersebut, akan mulai dilakukan persiapan dan proses terkait lainnya dalam rangka pemutusan tersebut.

Kebijakan VPN

a. Koneksi ke dalam jaringan internal Danareksa yang berasal dari luar tanpa pengecualian harus dilakukan dengan menggunakan layanan VPN yang disediakan.
b. Pihak IT menetapkan daftar pengguna yang dapat melakukan akses ke jaringan Danareksa melalui VPN. Penambahan atau pengurangan ke daftar ini harus dilakukan melalui permintaan secara formal dan tercatat, dengan persetujuan kepala unit kerja pengguna yang bersangkutan. Pihak IT akan melakukan penambahan atau pengurangan yang diminta setelah semua proses persetujuan dilengkapi.
c. Dalam kasus khusus tertentu, atau dalam keadaan mendesak, kepala unit kerja dapat meminta secara langsung kepada IT agar akses pengguna tertentu dikeluarkan dari daftar di atas, dimana kelengkapan proseduralnya dapat disusulkan maksimal dalam 5 hari kerja kemudian.

d. Koneksi melalui VPN oleh individual Danareksa harus dilakukan dengan menggunakan perangkat keras dan lunak yang sesuai dengan standar yang ditetapkan Danareksa.
e. Koneksi melalui VPN oleh individual Danareksa paling baik dilakukan dengan menggunakan "one-time password' seperti dengan token (*synchronous* atau *asynchronous*) ataupun sistem *public/private key* dengan teknologi PKI (*Public- Key Infrastructure*),
f. Implementasi sistem di atas dapat dilakukan secara bertahap, dimana pada tahap awalnya dapat digunakan sistem sementara berupa autentifikasi dengan menggunakan *username* dan *password*. Jika cara ini digunakan, maka autentifikasi harus dilakukan dengan sistem yang terpisah dari sistem autentifikasi jaringan internal Danareksa, dan disertai dengan dengan rencana implementasi dan transisi dari sistem sementara ke sistem yang telah ditetapkan di atas.
g. Komputer individual (*notebook* ataupun PC) yang tersambung ke jaringan Danareksa melalui VPN harus mengaktifkan VPN *tunnel* dari *software* yang telah di-*install*, dimana *tunnel* ini akan menonaktifkan koneksi ke jaringan lainnya yang dimiliki oleh komputer termaksud.
h. Komputer individual yang tersambung ke jaringan Danareksa melalui VPN harus memiliki *software* antivirus yang aktif dan *up-to-date*, sehingga meminimalkan risiko kornputer tersebut sudah terkena virus saat melakukan koneksi ke jaringan Danareksa. *User* bertanggung jawab penuh jika komputernya menjadi sumber serangan virus ke jaringan Danareksa saat menggunakan koneksi VPN yang ada.
i. Koneksi VPN individual akan dipantau secara *software*, dan jika tidak ada aktivitas jaringan selama 30 menit maka otomatis koneksi tersebut diputus. Hal ini tidak berlaku untuk koneksi VPN dari satu lokasi kantor Danareksa ke kantor lainnya,
j. Koneksi VPN individual ke jaringan internal Danareksa harus melakukan autentifikasi ulang setiap 30 menit, dimana diberikan tenggang waktu selama 5 menit bagi pengguna layanan untuk memenuhi proses ini. Jika di akhir tenggang waktu tersebut proses belum selesai, maka secara otomatis koneksi akan diputus, dan harus dilakukan koneksi ulang.
k. Koneksi VPN individual untuk mengakses layanan tertentu di DMZ tidak diharuskan melakukan autentifikasi ulang ini. Namun diberikan batasan maksimal lamanya koneksi adalah 8 jam. Jika koneksi tanpa autentifikasi ulang sudah mencapai 8 jam, maka koneksi akan diputus dan harus dilakukan koneksi ulang.
l. Secara umum, komputer yang digunakan untuk meng-akses jaringan Danareksa melalui layanan VPN ini harus memenuhi dan mematuhi semua kebijakan Danareksa mengenai teknologi dan informasi, serta keamanan dan keselamatan.
m. Pihak IT berhak untuk menetapkan jenis layanan yang dapat diakses melalui jaringan jenis layanan baru yang perlu diakses melalui VPN, maka dilakukan proses perubahan jenis akses tersebut secara formal dan tercatat, yang akan disetujui oleh pihak IT dan kepala unit kerja yang bersangkutan.

n. Setiap *User* yang melakukan koneksi melalui VPN bertanggung jawab atas semua transaksi yang dilakukan selama koneksi terjadi. Pihak IT akan memberikan catatan koneksi dan transaksi sebagai bukti jika diperlukan klarifikasi.
o. Jika dideteksi *User* melakukan pelanggaran atas hak dan kewajibannya dalam menggunakan koneksi VPN ke jaringan Danareksa, maka akan dilakukan penghapusan hak koneksi atas nama *User* tersebut. Jika diperlukan, dan berdasarkan hasil investigasi atas pelanggaran yang terjadi, dapat diberikan tindakan disipliner terhadap user tersebut, yang dapat berupa sanksi administratif ataupun pemberhentian pegawai yang bersangkutan.

X.3. Jaringan Intranet (*Wire Network*)

Tujuan

Mengatur jaringan internal Danareksa agar berfungsi secara optimal, serta sesuai dengan standar jaringan yang fleksibel, aman, dan mudah dari segi administrasi dan pemeliharaan jaringan.

Ruang Lingkup

Seluruh jaringan di lokasi operasional Danareksa, termasuk perangkat keras dan lunak yang terlibat.

Tanggung Jawab

Pihak IT akan melakukan pengawasan terhadap operasional perangkat keras dan lunak dalam rangka penyediaan layanan jaringan Danareksa.

Kebijakan

a. Seluruh perangkat keras yang digunakan untuk penyediaan jaringan Danareksa harus dilindungi dengan sistem catu daya darurat UPS, dimana dapat digunakan UPS secara terpusat ataupun untuk masing-masing perangkat. Catu daya baterai yang disediakan oleh UPS tersebut harus lebih dari 10 menit dan cukup untuk menghindarkan perangkat tersebut agar tidak mati secara mendadak.
b. Jaringan Danareksa harus dikonfigurasikan secara paling handal, untuk mencapai tingkat kualitas layanan sebesar 98% "uptirne." Untuk cara pengukuran dan parameter lainnya yang digunakan akan ditentukan dalam dokumentasi SLS jaringan secara terpisah.
c. Seluruh perangkat keras yang digunakan untuk penyediaan jaringan Danareksa harus dilindungi dengan suatu sistem pemeliharaan berkala (*preventive maintenance*), baik yang dilakukan sendiri, oleh vendor perangkat, ataupun oleh pihak ketiga lainnya. Perbaikan kerusakan, *upgrade*, atau penggantian perangkat harus tetap mengindahkan target kualitas layanan yang telah ditetapkan di atas.

d. Untuk perangkat yang dianggap sangat vital bagi ketersediaan layanan, maka harus dipersiapkan perangkat cadangan sebagai "standby unit' yang dapat diaktifkan dalam waktu singkat.
e. Sistem perkabelan (*structured cabling system*) yang digunakan oleh Danareksa harus disesuaikan dan disertifikasi menurut standard CAT6, dengan garansi dari vendor minimum selama 15 tahun sejak instalasi. Diagram dan dokumentasi sistem perkabelan dan sertifikasinya harus terdokumentasi dan diarsip dengan baik.
f. Sistem perkabelan yang sama juga akan menjadi jalur jaringan telepon Danareksa, serta jalur komunikasi data lainnya, yang harus dipisahkan dari jaringan IT Danareksa.
g. Jaringan internal Danareksa akan berupa *"fully-switched environment"* yang berarti menggunakan perangkat switch sebagai access concentrator-nya. Perangkat *"shared hubs"* tidak boleh dipergunakan lagi, kecuali untuk jaringan di dalam ruang training atau ruang yang penggunaannya bersifat sementara, dan dimana seluruh perangkat kornputer yang dikoneksi kepada shared hub tersebut digunakan atau dimiliki oleh satu orang pengguna jaringan.
h. Akses secara fisik ke tempat-tempat dimana *"shared hubs"* masih dipergunakan harus diatur dan dijaga agar akses oleh pihak luar tidak dimungkinkan tanpa pengawasan oleh pihak internal Danareksa.
i. Sistem jaringan Danareksa akan menggunakan konsep *"collapsed backbone"* dimana perangkat switch sebagai access concentrator akan terbagi menjadi tiga fungsi secara hirarkis, sebagai *"core," "distribution,"* dan *"access."* Perangkat *"core"* berfungsi sebagai pusat interkoneksi jaringan, yang menghubungkan beberapa jaringan distribusi, dan menghubungkan jaringan server; perangkat "distribusi" membagi jaringan Danareksa menjadi beberapa *"enclave"* misalnya pemisahan untuk masingmasing lantai atau bagian kantor Danareksa, sedangkan perangkat *"access"* adalah perangkat yang langsung berhubungan dengan PC dan perangkat user lainnya. Pemisahan hierarkis ini dilakukan agar terjadi segmentasi jaringan yang optimal.
j. Jarak antara perangkat *core* dan setiap PC di Danareksa dijaga maksimal 4 hop. Untuk lokasi selain kantor pusat, maka jarak 4 hop tersebut adalah dari perangkat router paling luar yang terdekat dengan PC di lokasi tersebut.
k. Perangkat keras jaringan *(switch, router,* dan lain-lain) yang digunakan di jaringan internal Danareksa harus dapat dikontrol dari satu tempat yang terpusat, dengan suatu perangkat lunak *Network Management System* (NMS). Perangkat NMS ini harus dapat memperlihatkan secara realtime informasi loading dan konfigurasi perangkat jaringan di atas. Perangkat NMS ini juga harus dapat mencakup seluruh perangkat jaringan yang digunakan di Danareksa, dalam fungsi monitoring dan konfigurasinya.
l. Jika perangkat NMS mengindikasikan terjadinya gangguan layanan, maka IT harus segera menanganinya, sesuai dengan SLA layanan yang telah disetujui secara terpisah. Jika diperkirakan bahwa gangguan akan berlangsung selama lebih dari 30 menit, maka pihak IT wajib membuat pemberitahuan kepada ISO dan semua

pengguna layanan terkait, paling tidak dalam bentuk email. Jika gangguan terjadi di lokasi dimana tidak ada akses email, maka pemberitahuan diberikan ke pejabat yang telah ditunjuk. Pemberitahuan tersebut minimal memuat jenis gangguan dan kemungkinan lamanya gangguan terjadi.

m. Perangkat keras jaringan *(switch, router,* dan lain-lain) yang digunakan di jaringan internal Danareksa harus beroperasi dengan tingkat utilisasi rata-rata maksimal 80%; jika' tingkat ini sudah dicapai maka harus direncanakan untuk dilakukan upgrade dengan perangkat yang kapasitasnya lebih besar. Data mengenai tingkat utilisasi ratarata ini didapat dari laporan realtime perangkat lunak NMS yang digunakan. Pihak internal IT dapat mengundang ISO untuk ikut rnelakukan review kinerja perangkat keras jaringan tersebut.
n. Semua catatan, dokumentasi dan diagram konfigurasi dari perangkat jaringan dan jaringan Danareksa sendiri harus didokumentasikan secara konsolidasi dan terstruktur. Jika terjadi perubahan atas jaringan dan perangkat jaringan maka catatan, dokumentasi dan diagram konfigurasinya harus disesuaikan paling lambat 2 (dua) minggu setelah perubahan terjadi. Akses terhadap catatan ini terbuka untuk pihak IT, ISO, IRT. Akses untuk pihak terkait lainnya akan diberikan jika diperlukan.

X.4. Pemeliharaan Perangkat *Routing* dan *Switching*

Tujuan

Konfigurasi minimal yang harus dilakukan ke perangkat keras dan lunak yang melakukan fungsi *routing* dan *switching* di jaringan Danareksa, termasuk *cable concentrator*, untuk mencapai kinerja yang optimal dan tingkat keamanan yang dipersyaratkan.

Ruang Lingkup

Seluruh perangkat keras dan lunak yang menjalankan fungsi *routing* dan *switching*, termasuk *cable concentrator*, yang berada di lingkup jaringan Danareksa, kecuali, perangkat yang berada di dalam DMZ, yang sudah tercakup dalam kebijakan tersebut di atas.

Tanggung Jawab

a. Pihak IT akan melakukan pemeliharaan perangkat yang tercakup untuk memenuhi kebijakan ini, dan memastikan kinerja perangkat sesuai dengan SLA/SLS yang telah ditetapkan.
b. Pihak IT akan melengkapi segala dokumentasi, diagram, detail konfigurasi, dan pengalamatan perangkat yang tercakup, dan menyimpannya secara terpusat untuk memudahkan akses ke informasi ini bila diperlukan.

c. Pihak IT akan bekerja sama dengan ISO dimana diperlukan, dalam rangka ikut mengamankan informasi perusahaan.
d. Pihak IT akan terus memantau perkembangan teknologi yang terjadi, dan melakukan usulan perubahan konfigurasi ataupun perangkat sesuai dengan kebutuhan perusahaan

Kebijakan

a. Semua perangkat *routing* dan *switching* harus di-*set up password* untuk akses dan *password* untuk administratornya, sehingga akses ke perangkat tersebut terbatas hanya untuk pihak yang berwenang seperti IT saja.
b. *Password* administratif dari semua perangkat di atas akan dikelola oleh IT dengan menggunakan sistem *tellkey box*, untuk memungkinkan akses dalam keadaan darurat.
c. Semua perangkat *routing* dan *switching* harus memiliki cara untuk kontrol administratif secara jarak jauh, dengan menggunakan protokol yang aman seperti SSH atau HTTPS.
d. Semua perangkat di atas harus menampilkan DISCLAIMER standar yang telah ditetapkan Danareksa. Secara minimum DISCLAIMER ini harus menyatakan bahwa akses ke perangkat di atas oleh pihak-pihak selain yang berhak dan berkepentingan adalah ilegal dan dilarang.
e. Semua perangkat di atas harus memiliki sistem *backup* yang terpusat, dimana perangkat yang bermasalah dapat ditangani atau digantikan dengan cepat, lengkap dengan spesifikasi dan konfigurasi yang diperlukan.
f. Pihak IT harus merencanakan kontrol administratif yang terpusat, seperti menggunakan suatu perangkat lunak NMS (*Network Management System*). Jika NMS sudah digunakan, pada perangkat *routing* dan *switching* tidak diperbolehkan ada user database yang bersifat lokal di perangkat.
g. Semua perangkat *routing* dan *switching* harus memiliki fitur protokol SNMP untuk dapat dilakukan polling secara periodik. Untuk semua perangkat di atas akan dilakukan *setting community string* SNMP yang sudah ditetapkan Danareksa. Tidak diperbolehkan untuk menggunakan SNMP *community string* kosong " " atau *set up default*-nya. Lalu lintas SNMP ini harus dijaga hanya untuk jaringan internal Danareksa, dan dilakukan *blocking* pada *firewall* Danareksa.
h. Pihak IT akan menggunakan suatu *softwar*e standar untuk menerima dan menampilkan hasil *polling* tersebut, yang dapat digunakan untuk pelaporan kinerja ataupun loading yang dialami oleh perangkat-perangkat tersebut, yang berkaitan dengan SLA/SLS yang telah disepakati. Pihak IT akan selalu menjaga kinerja dan *loading* yang dialami oleh perangkat di atas sesuai dengan SLA/SLS yang telah ditetapkan.
i. Jika terjadi kinerja atau *loading* yang berada di luar SLA/SLS yang telah ditentukan, maka *software* tersebut dapat mengirimkan pemberitahuan kepada tim *support* perangkat, yang dengan segera menentukan tindakan yang harus diambil. Tindakan tersebut dapat berupa upaya perbaikan secara jarak jauh

ataupun langsung di lokasi, dan dapat berupa kerja sama dengan pihak ketiga jika merupakan layanan *outsource*.

j. Pihak penanggung jawab perangkat di atas akan bekerja sama dengan ISO untuk menentukan tingkat keamanan perangkat yang optimal. ISO akan memberikan informasi mengenai *hotfix/patch* yang tersedia dan siap untuk di-*install* ke perangkat, dan pihak penanggung jawab akan membuat jadwal instalasi yang dimungkinkan. ISO akan memberikan persetujuan atas jadwal tersebut, dan bilamana akan ada gangguan jaringan maka pemberitahuan akan diberikan sesuai dengan ketentuan yang berlaku.

k. Protokol yang berlaku di Danareksa adalah berbasiskan IP (*Internet Protokol*). Jika ada perangkat *routing* dan *switching* yang menggunakan protokol jenis lain (seperti IPX, SNA/SDLC, maupun NETBEUI), maka pihak IT harus memberikan catatan dan alasan mengapa protokol lainnya ini digunakan. Jika dianggap bahwa protokol tersebut dapat digantikan oleh protokol IP, maka protokol tersebut harus dihapus dari konfigurasi perangkat.

l. Beberapa jenis kegiatan jaringan di bawah ini harus diminimalkan, dan sedapat mungkin tidak diaktifkan pada perangkat *routing* yang digunakan oleh Danareksa:
   i. *Broadcast*, IP *directed broadcast* dan *multicast*;
   ii. TCP dan UDP *small services* (seperti: *echo*, *chargen*, *discard*, *daytime*)
   iii. LSRR (*Loose Source Record Routing*)
   iv. *Packet* dengan alamat pengirim diluar jaringan Danareksa
   v. *Port* SMTP, HTTP, dan port lainnya yang tidak digunakan pada perangkat tersebut.

m. Keseluruhan jaringan Danareksa akan dibagi menjadi beberapa *subnet* sesuai dengan pengelompokan yang sesuai, misalnya berdasarkan lantai gedung tempat lokasi fisik kornputer yang bersangkutan. Hal ini dilakukan untuk mengurangi risiko beban yang terlalu tinggi pada jaringan Danareksa.

n. Jika diperlukan, dapat dilakukan VLAN untuk suatu kelompok komputer tertentu yang mernerlukan tingkat kinerja dan keamanan yang lebih tinggi. Keperluan untuk konfigurasi jenis ini akan ditentukan oleh permintaan dari pegawai, keperluan operasional mereka, serta ketersediaan perangkat dan fiturnya. Pegawai yang membutuhkan konfigurasi semacam ini harus melalui suatu proses yang formal dan tercatat.

o. Jalur-jalur yang sifatnya penting untuk operasional Danareksa harus memiliki *standby backup* yang dapat segera menggantikan jalur utama. Konfigurasi untuk jalur *backup* ini dapat ditentukan sesuai dengan SLA yang telah ditetapkan, antara lain menggunakan *leased line*, ISDN *dial*, ataupun ADSL.

X.5. Jaringan Nirkabel

Tujuan

Mengatur koneksi ke dalam jaringan Danareksa dengan menggunakan media nirkabel, baik dengan standar 802.11x, maupun dengan standar serupa lainnya.

Ruang Lingkup

Seluruh jaringan di lokasi operasional Danareksa, yang berupa perangkat keras dan lunak yang dapat berfungsi untuk menerima atau membuat koneksi nirkabel.

Tanggung Jawab

Pihak IT akan melakukan pengawasan terhadap penggunaan perangkat nirkabel di lingkungan Danareksa, baik dengan menggunakan cara-cara konvensional atau fisik, atau dengan menggunakan teknologi.

Kebijakan

a. Koneksi jaringan nirkabel dibagi dua jenis, yaitu koneksi individual ke jaringan dengan menggunakan perangkat nirkabel, dan koneksi antar jaringan dengan media nirkabel.
b. Untuk saat ini, koneksi nirkabel jenis pertama yaitu koneksi individual PC atau *notebook* ke jaringan Danareksa tidak diperbolehkan. Jika perangkat PC atau notebook yang digunakan di lingkungan Danareksa mempunyai fasilitas nirkabel, maka fasilitas tersebut harus di non-aktifkan.
c. Penggunaan perangkat yang dapat menerima koneksi nirkabel individual (misalnya: *Access Point* 802.11a/b/g) di dalam lingkungan Danareksa untuk keperluan apapun, tidak diperbolehkan.
d. Koneksi nirkabel jenis kedua, yang menghubungkan dua jaringan dengan media nirkabel, masih diperbolehkan jika memang setelah dilakukan pertimbangan mendalam tidak tersedia pilihan lainnya secara efisien dan optimal.
e. Untuk koneksi jenis kedua di atas, diharuskan menggunakan media yang dilengkapi dengan enkripsi jalur, baik dengan metode standar (DES, AES) ataupun metode proprietary perangkat, yang telah terbukti aman. Pengiriman data dalam bentuk teks langsung (*clear text*) melalui media nirkabel, tidak diperbolehkan.
f. Koneksi nirkabel jenis kedua yang digunakan pada poin d dan e harus menghubungkan dua jaringan Danareksa. Jika terjadi koneksi nirkabel antara jaringan Danareksa dan jaringan eksternal, maka diberlakukan juga aturan seperti pada kebjijakan koneksi pihak ketiga.
g. Untuk koneksi nirkabel yang digunakan Danareksa, jika menggunakan protokol dengan frekuensi yang diatur, maka Danareksa harus mendapatkan secara legal dan tercatat hak atas frekuensi yang digunakan di perangkat nirkabel. Gangguan frekuensi atau interferensi baik yang ditimbulkan maupun yang diterima oleh perangkat harus ditekan seminimal mungkin.
h. Penggunaan perangkat jaringan tersebut di atas harus sesuai dengan segala peraturan perundangan yang berlaku. Jika dibutuhkan audit ataupun pemeriksaan

oleh pihak yang berwenang, maka pihak internal Danareksa harus membantu dan melakukan persiapan yang dibutuhkan.

X.6. Pemeliharaan Layanan Domain Internet Danareksa

Tujuan

Mengatur pemeliharaan nama domain yang dimiliki dan digunakan oleh Danareksa, serta layanan Internet yang disediakan oleh Danareksa melalui domain tersebut.

Ruang Lingkup

Seluruh layanan Internet Danareksa dan komponen-komponennya, seperti *e-mail server*, *name server*, *proxy server*, dan lainnya.

Tanggung Jawab

Pihak IT akan melakukan pengawasan terhadap layanan yang diberikan oleh domain-domain Danareksa, baik kepada pengguna eksternal maupun internal.

Kebijakan

Danareksa memiliki beberapa domain Internet yang masing-masingnya harus mempunyai konfigurasi minimum sebagai berikut:

a. Domain tersebut diregistrasikan atas nama PT Danareksa (Persero) atau Anak Perusahaan.
b. Memiliki paling tidak dua DNS *server* untuk setiap domain.
c. Memiliki kontak administratif dan teknis berupa suatu pihak internal Danareksa sendiri, atau pihak ketiga yang sesuai dengan perjanjian yang dimiliki oleh Danareksa.
d. Pengadaan domain baru selain dari yang di atas harus diusulkan oleh unit kerja terkait dengan pihak IT untuk mendapat persetujuan Direksi Penanggungjawab IT dan Direksi yang membawahi Divisi yang mengajukan permintaan.
e. Pengeloiaan registrasi domain harus terjaga tetap aktif, dimana seluruh kewajiban baik Danareksa ataupun pihak ketiga atas domain tersebut dipenuhi pada waktunya.
f. Untuk domain-domain lainnya yang dimiliki Danareksa, maka sedapat mungkin layanan disediakan oleh pihak yang sama dengan domain utama Danareksa, dan berlaku SLA yang sama.
g. Jika terjadi perubahan layanan pihak ketiga mengenai domain ini, maka Danareksa harus segera melakukan perubahan dan dengan persiapan memadai agar dampak perubahan ini minimal pada pemeliharaan domain Danareksa.

h. Ditentukan suatu fungsi Webmaster sebagai kontak utama Danareksa dengan pihak ketiga pengelola domain Danareksa terkait.

Kebijakan DNS Domain Danareksa

a. Paling tidak harus ada dua DNS *server* untuk setiap domain Danareksa, dengan konfigurasi ideal dimana paling tidak satu dari kedua *server* tersebut dilindungi oleh suatu SLA, misalnya berada pada pihak ketiga yaitu penyedia layanan Internet (ISP) untuk Danareksa.
b. Jika terjadi perubahan ISP, maka Danareksa harus segera melakukan perubahan dan dengan persiapan memadai agar dampak perubahan ini minimal pada layanan *name service* untuk domain Danareksa.
c. Danareksa, dalam hal kebijakan ini diwakili oleh pihak IT, harus memastikan bahwa narna-nama *server* yang sudah diregistrasikan dalam domain dengan memiliki *record* "forward' dan "reverse" nya yang saling sesuai.
d. Konfigurasi SOA (*Source of Authority*) untuk domain Danareksa harus memiliki paling tidak data sebagai berikut:
    i. Primary NS adalah salah satu dari kedua *server* DNS yang ditentukan sesuai huruf a.
    ii. Kontak untuk "responsible administrator" berupa suatu *email address* yang diawaki dan dimonitor dengan baik.
    iii. *Setting* untuk *refresh* sebesar 10.800 detik (3 jam)
    iv. *Setting* untuk *retry* sebesar 3.600 detik (1 jam)
    v. *Setting* untuk *expiration* sebesar 259.200 detik (3 hari)
e. Untuk seluruh domain Danareksa berlaku SLA yang sama mengenai "uptime" dari layanan DNS yang diberikan aleh ISP yang ditentukan di poin 1.
f. Untuk pengguna internal Danareksa ditetapkan dua DNS *server* yang akan digunakan. Kedua *server* internal ini harus dipelihara sebaik mungkin, dengan *record* "forward' dan "reverse" dari kedua *server* yang saling sesuai.
g. Danareksa menerapkan "split horizon DNS" untuk kedua pasang *server* internal dan eksternal, untuk memastikan agar hanya DNS *record* untuk *server* yang terbuka di Internet fah yang dapat diakses dari Internet.
h. *Database* DNS internal dan eksternal tersebut harus terpelihara dengan baik, dan *record* yang sama pada *database* tersebut menghasilkan informasi yang sama pula.
i. Keamanan informasi yang tertera di DNS harus dijaga terutama untuk *server* yang terbuka ke arah Internet.

Kebijakan E-mail Domain Danareksa

a. Layanan e-mail untuk domain Danareksa harus menggunakan sedikitnya dua e-mail *server* yang berbeda.
b. Kedua *server* di atas diatur dengan prioritas utama *server* milik Danareksa yang berada di dalam DMZ, dan *server* kedua harus digunakan *server* milik ISP yang

berguna sebagai tempat penyimpanan e-mail sementara jika e-mail *server* utama domain Danareksa terganggu layanannya.

c. Konfigurasi kedua *server* tersebut harus seperti di bawah ini:
   i. domain Danareksa MX 10maildana.domain Danareksa [*server* internal]
   ii. domain Danareksa MX 20 corp3.cbn.net.id [*server* eksternal]
d. Kedua e-mail *server* tersebut tidak boleh berfungsi sebagai *Open Main Relay* dan hanya menangani domain Danareksa saja.

Kebijakan *Server* Domain Danareksa

a. Semua layanan yang diberikan kepada pengguna internal dan eksternal Danareksa menggunakan perangkat keras *server* yang harus mengacu pada standar di bawah ini:
   i. Server OS yang digunakan minimal 1 (satu) versi dibawah versi OS terbaru/terakhir dan masih mendapatkan dukungan layanan dari prinsipal atau vendor.
   ii. *Platform* yang digunakan adalah berbasiskan prosesor Intel 32-bit atau 64-bit, tetapi tidak ditutup kemungkinan *platform* berbasiskan prosesor lainnya yang dapat secara handal menjalankan OS di atas.
   iii. *Hard disk* dengan *interface* paling tidak FW SCSI atau versi yang lebih baru, yang mampu memberikan layanan RAID (*Redundant Array of Inexpensive Disks*) level 0 sampai 5, dengan konfigurasi pilihan RAID 0+1.
   iv. Jika diperlukan, menggunakan eksternal *storage* yang berbasiskan *Fiber Channel* atau iSCSI.
   v. *Network card* dengan kapasitas 1GB *full duplex* (media GBIC atau UTP), tersambungkan ke *switch* yang dapat menangani jaringan GB.
   vi. Ketersediaan fitur untuk *redundant fan* dan *redundant power supply unit*, untuk menjaga ketersediaan (*uptime*) *server* tersebut diutamakan.
   vii. Spesifikasi lainnya yang dipandang perlu, dan ditentukan oleh IT saat pengadaan *server* tersebut.

b. Untuk spesifikasi yang lebih rendah dari di atas, maka harus dibuat penjelasan dan justifikasi mengenai penggunaan *server* tersebut, dengan sepengetahuan IT.
c. Setiap *server* yang digunakan oleh Danareksa harus secara rutin melakukan *patching* sesuai dengan jadwal yang ditentukan oleh IT. Sebelum instalasi dilakukan pihak IT harus yakin bahwa instalasi tidak akan mengurangi tingkat kinerja *server* tersebut.
d. Untuk konfigurasi *update/patch* secara otomatis dari Microsoft harus tersedia suatu *platform*, misalnya dengan SUS (*Server Upgrade Services*) ataupun WUS (*Windows Update Services*). Semua PC dan *notebook* Danareksa akan mendapatkan *update/patch* dari *server* ini secara otomatis.
e. Pihak IT tetap harus melakukan monitoring atas status dari *upgrade* yang terjadi untuk menentukan apakah suatu intervensi ataupun *patching* secara manual perlu untuk dilakukan.

f. Kriteria kinerja *server* yang digunakan di Danareksa harus mengacu pada parameter di bawah ini, sesuai dengan *standard best practice* Microsoft.

Object	***Counter***	***Interval***	***Threshold***	***Description***
Logical Disk	*Free Megabytes*	*Every* 15 *min*	<10% of **logical disk size**	*Megabytes* yang masih tersisa di *hard disk* yang ada, jika tersisa kurang dari 10% merupakan risiko data yang tidak dapat disimpan ke *disk* karena *disk* sudah penuh.
Memory	*Available Megabytes*	*Every 15 min*	4 MB	Jika jumlah *memory* yang tersedia turun dibawah 4 MB, maka ada risiko sistem akan kekurangan *memory*, yang dapat mengakibatkan kegagalan sistem.
Memory	*Page Faults / sec*	*Every* 5 *min*	700 / s	Tingginya jumlah *faults* menunjukkan kurangnya *physical memory*.
Physical Disk	*Current Disk Queue Lenght*	*Every 1 min*	*2 Averaged over 3 intervals*	Untuk *hard disk* yang memuat DIT dan *log files*, jika *queue* terlalu panjang maka perlu peningkatan kinerja *disk* sistem.
Processor	*% DPC Time_Total (instance)*	*Every 15 min*	10	*Task Deffered Procedure Calls* (DPC) yang diterima dan diproses oleh CPU, untuk menunjukkan rata-rata waktu proses dan waktu tunggu CPU.
Processor	*% Processor Time_Total*	*Every 1 min*	*85% Averaged over 3 intervals*	*Processor Time* di atas 85% menunjukkan *overloading* CPU, untuk mengetahui proses mana yang paling banyak menggunakan CPU, dapat dilihat dari

				parameter "% Processor Time-Process Name".
System	*Context Switches / sec*	*Every 15 min*	70,000	Angka yang terlalu tinggi menunjukkan terlalu banyak terjadi *switching* antara satu aplikasi ke aplikasi lainnya, yang banyak menimbulkan *overhead* ke sistem.
System	*Processor Queue Lenght*	*Every 1 min*	*6 Averaged over 5 intervals*	CPU tidak cukup cepat kinerjanya sehingga terjadi antrian proses. Jika angka terlampaui maka dapat dipertimbangkan *upgrade* CPU.
System	*System Up Time*	*Every 15 min*	> 98%	Ukuran dari ketersediaan dan kehandalan sistem.

g. *Server* yang digunakan harus dapat secara periodik memberikan data kinerja-nya kepada sistem NMS yang digunakan. Pihak IT harus melakukan suatu *capacity planning*, dan melakukan monitoring atas kinerja *server* sesuai dengan parameter yang ditentukan. Jika ditemukan satu perangkat keras yang secara konsisten beroperasi di luar batasan yang telah ditentukan di atas, maka harus direncanakan suatu *upgrade* perangkat keras yang akan dikoordinasikan oleh IT.
h. Untuk mengoptimalkan jumlah data yang harus disimpan, maka dimungkinkan untuk melakukan monitoring parameter-parameter yang dianggap kritis dan penting, dan monitoring secara lebih detail akan dilakukan jika dideteksi terjadi anomali pada kinerja sistem yang dimonitor, dengan menggunakan sistem monitoring yang dapat melakukan monitoring dari semua parameter yang tersebut di atas.
i. Untuk mengoptimalkan jumlah data yang harus disimpan, maka NMS akan melakukan akumulasi data kinerja tersebut secara harian, dimana setelah itu data detail dapat dihapuskan. Interval waktu penghapusan data detail ini akan ditetapkan secara prosedural oleh pihak IT.
j. Untuk semua layanan IT yang diberikan oleh Danareksa, baik untuk pengguna internal ataupun eksternal, harus direncanakan untuk melakukan audit, baik audit kinerja, audit *compliance* ataupun audit keamanan dan keselamatan, paling tidak satu kali dalam satu tahun. Kegiatan audit ini akan dikoordinasikan oleh Internal Audit.

X.7. Pemeliharaan *Database*

Tujuan

Mengatur pemeliharaan data dan informasi yang tersimpan dalam sistem *database* di Danareksa.

Ruang Lingkup

Seluruh sistem *database* dan penyimpanan data lainnya yang digunakan di layanan Danareksa, baik yang internal ataupun eksternal.

Tanggung Jawab

a. Pihak IT akan menunjuk satu fungsi DBA *(Database Administrate')* yang akan melakukan pengawasan dan pengamanan terhadap layanan berbasis informasi yang diberikan oleh Danareksa, baik kepada pengguna eksternal maupun internal.
b. Pihak pengembangan aplikasi berkoordinasi dengan DBA dalam hal desain, instalasi, dan persiapan *database* untuk sistem aplikasi yang sedang dikembangkan, serta dalam kebutuhan data untuk *testing* dan kegiatan lainnya selama proses pengembangan.
c. Pihak pengelola aplikasi yang menggunakan sistem *database* tersebut berkoordinasi dengan DBA dalam melakukan pemeliharaan data aplikasi yang tersimpan dalam sistem *database* tersebut.

Kebijakan

a. Sistem *database* yang digunakan oleh IT harus memenuhi standar di bawah ini:
    i. Berbasiskan *Relational Database Management* (RDMS) yang umum dan terbukti digunakan di industri IT, minimal 1 (satu) versi dibawah versi *database* yang terbaru/terakhir dan masih mendapatkan dukungan layanan dari prinsipal atau vendor sistem *database*.
    ii. Memiliki CAL yang sesuai dengan jumlah akses.
    iii. Memiliki lisensi sesuai dengan ketentuan lisensi yang berlaku.
    iv. RAM ter-*install* harus sesuai atau lebih dari rekomendasi yang diberikan, terutama untuk menjaga parameter *Page Fault* per detik di bawah ambang yang telah ditentukan
    v. Spesifikasi lainnya yang dipandang perlu, dan ditentukan oleh IT saat instalasi sistem *database* tersebut.
b. Untuk sistem *database* yang sudah berjalan dan belum memenuhi kriteria di atas, maka pihak IT harus mempersiapkan penjelasan dan rencana implementasi untuk mencapai ke arah standar yang ditetapkan di atas. Implementasi tersebut

harus selesai diterapkan tidak lebih dari satu tahun sejak rencana tersebut disetujui.

c. Aplikasi *database* minimal harus menggunakan konsep pemrograman 3-tingkat (*three-tier application*) dimana akses ke sistem *database* dilakukan oleh program aplikasi di *server*, dan tidak ada aplikasi di *user* yang langsung melakukan akses ke sistem *database*, baik untuk *read/write* maupun secara *read-only*.
d. Sistem autentifikasi *user database* dan sistem kontrol akses akan mengacu pada suatu daftar *user* yang terpusat, yang dapat diletakkan pada sistem *Active Directory Microsoft*, atau sistem terpilih lainnya yang sejenis dan setara. Sistem *database* yang digunakan tidak boleh memiliki daftar *user* sendiri-sendiri dan harus menggunakan daftar *user* terpusat ini. Sistem pengembangan aplikasi dan Domain Danareksa termasuk harus menggunakan autentifikasi berdasarkan daftar *user* terpusat ini.
e. Jika hal di atas tidak dapat dipenuhi, maka pihak IT atau pihak yang bertanggung jawab atas *database* atau aplikasi yang digunakan harus melakukan pelaporan eksepsi atas kebijakan ini, yang dilengkapi dengan rencana untuk perbaikan ke arah standar yang ditetapkan. Rencana perbaikan tersebut memuat jadwal implementasi yang tidak lebih dari dua tahun sejak eksepsi dibuat dan disetujui.
f. Daftar *User* terpusat di atas harus dipisahkan antara *User* yang merupakan pegawai Danareksa dan memang dipergunakan untuk operasionalnya sehari-hari, dengan *User* yang bersifat sementara seperti *User* yang dipergunakan untuk pengembangan aplikasi, dan *User* yang bersifat eksternal (pengguna domain Danareksa). Pemisahan ini dapat dilakukan dengan penggunaan *grouping* yang berbeda,
g. Sistem *database* untuk kegiatan pengembangan harus dipisahkan dari sistem *database* untuk kegiatan operasional, lengkap dengan sistem akses kontrol tersendiri, dan administrator yang berlainan. Sistem *database* operasional tidak boleh digunakan untuk kegiatan pengembangan, baik yang sifatnya pemrograman ataupun *testing*.
h. Secara berkala dilakukan kegiatan audit terhadap sistem *database* ini, yang akan dikelola oleh unit kerja Internal Audit, dan minimal meliputi audit terhadap kinerja dan kearnanan *database*, termasuk audit terhadap daftar *user* dan daftar akses yang dimilikinya.
i. Sernua aplikasi *database* memiliki administrator tersendiri yang bertugas untuk memelihara aplikasi tersebut. Administrator ini merupakan *support* utama dari aplikasi yang berjalan tersebut, dan akan bekerja sama dengan DBA dalam memelihara serta mendukung sistem aplikasi *database* secara keseluruhan.
j. Administrator aplikasi juga bertugas untuk menjaga kinerja dan keamanan operasional aplikasinya, baik dengan pengamanan standar seperti *user profile* dan kontrol akses, maupun dengan pengamanan *data entry* seperti *buffer overrun protection sena input validation*, dan cara-cara lainnya yang dirasa perlu.

k. Setiap *database* yang ter-*install* harus memenuhi tingkat kinerja yang dipersyaratkan dalam SLA/SLS yang telah dibuat untuk aplikasi *database* tersebut, terutama apabila aplikasi tersebut dianggap sebagai aplikasi utama atau aplikasi kunci dalam operasional Danareksa.

l. Tingkat kinerja yang dipersyaratkan tersebut dapat meliputi beberapa atau semua parameter di bawah ini:
   i. Konfigurasi awal *database* sudah menggunakan jumlah *resource* seperti prosesor, *memory* (baik fisik maupun virtual), dan kapasitas penyimpanan data secara maksimal.
   ii. Prosesor baik secara keseluruhan maupun khusus untuk proses SQL server, harus di bawah angka yang ditetapkan pada butir H.6.
   iii. Parameter *memory* yang harus dimonitor (jika tidak terdapat data *threshold* maka digunakan data historis untuk mengetahui keadaan yang diluar normal):

Object	***Counter***	***Interval***	***Threshold***	***Description***
Memory	*Available Bytes*	*Every 15 min*	4 MB	Sudah dilakukan sejalan dan mengambil data yang dihasilkan.
SQL Server: Memory Manager	*Connection Memory (KB)*	*Every 15 min*		Total memory dari *server* yang digunakan untuk mengatur koneksi ke *database*.
SQL Server: Memory Manager	*Lock Memory (KB)*	*Every 15 min*		Total *memory* dari *server* yang digunakan untuk mengatur *locks*.
SQL Server: Memory Manager	*Maximum Workspace Memory (KB)*	*Every 15 min*		Ukuran maksimum *memory* yang digunakan untuk menjalankan semua proses *database*.
SQL Server: Memory Manager	*Optimizer Memory (KB)*	*Every 15 min*		Total *memory* dari *server* yang digunakan untuk mengatur optimisasi *query*.
SQL Server: Memory	*SQL Cache Memory (KB)*	*Every 15 min*		Total *memory* dari *server* yang digunakan untuk mengatur *SQL cache*.

Manager				
SQL Server: Memory Manager	*Total Server memory (KB)*	*Every 15 min*		Total keseluruhan *memory* dari *server* yang digunakan untuk *database* tersebut.

iv. Parameter SQL *Server* yang harus dimonitor:

Object	***Counter***	***Interval***	***Threshold***	***Description***
SQL Server: General Statistics	*User Connections*	*Every 15 min*		Jumlah koneksi *User* pada saat yang bersamaan; *database* melakukan alokasi *resource* untuk masing-masing koneksi, dan konfigurasi untuk terlalu banyak *User* yang mengakibatkan *database* menggunakan *resource* yang besar.
SQL Server: Cache Manager	*Cache Hit Ratio*	*Every 15 min*	< 90%	Perbandingan *cache hits* dan *lookups* dari SQL *Server*, harus diatas 90%.
SQL Server: Databases	*Transactions/ sec*	*Every 15 min*		Jumlah transaksi per detik baik untuk masing-masing *database* maupun keseluruhan.
SQL Server: SQL Statistics	*SQL Recompilati-on/sec*	*Every 15 min*		Jumlah rekompilasi *query* dilakukan oleh *server*, harus dijaga serendah mungkin.
Process	*Thread Count*	*Every 15 min*		Jumlah *thread* untuk setiap *instance database*.

Disk I/O counters		*Every 15 min*		Jumlah *disk* I/O yang berlangsung pada setiap saat.
SQL Server: Databases	*Data File(s) Size (KB)*	*Every 15 min*		Ukuran *file database*, dan juga tempdb dan msdb untuk selalu dimonitor untuk mendapatkan data pertumbuhan ukuran *file-file* tersebut.

Object	***Counter***	***Interval***	***Threshold***	***Description***
SQL Server: Locks	*Number of Deadlocks/ sec*	*Every 15 min*		Jumlah *deadlock* yang terjadi setiap saatnya.
SQL Server: Databases	*Log file (s) Size (KB) and/or Log File(s) Used Size (KB)*	*Every 15 min*		Ukuran *log file*, baik secara fisik maupun kebutuhan *disk space*-nya.
SQL Server: Buffer Manager	*Procedure Cache Pages*	*Every 15 min*		Jumlah *page* yang digunakan untuk menyimpan *compiled queries*.
SQL Server: Buffer Manager	*Total Pages*	*Every 15 min*		Jumlah *page* yang dikonfigurasikan pada *buffer pool* (termasuk untuk *database*, *free* dan *stolen pages*).
SQL Server: Cache Manager	*Cache Pages*	*Every 15 min*		Jumlah halaman (dengan ukuran 8 KB) yang digunakan untuk *cache*.

v. Kinerja sistem dan I/O *disk*-nya sebagai berikut:

Object	***Counter***	***Interval***	***Threshold***	***Description***
Physical	*% Disk time*	*Every 15*		Prosentase waktu dimana

Disk		*min*		disk sedang bekerja untuk *read/write* data.
Physical Disk	*Average disk queue length*	*Every 15 min*		Panjang *queue* baik *read/write* yang menunggu karena *disk* sedang melakukan proses yang lain.
Physical Disk	*Average disk read/sec and Average disk white/sec*	*Every 15 min*		Jumlah prose read/write yang berlangsung pada setiap saat.

vi. Penggunaan *database index* secara optimal, dimana kolom-kolom yang sering digunakan dalam membentuk *query* pada *database* tersebut, terutama yang menggunakan klausa WHERE, ORDER BY, GROUP BY, TOP, dan DISTINCT, sudah dibuat *index*-nya. Penggunaan *index* ini akan ditinjau kembali secara periodik, untuk menjaga optimalitas kinerja *database*.

vii. Pengaturan proses *batch* yang dijadwalkan untuk dapat mengoptimalkan penggunaan *resource* sistem yang ada.

m. Untuk mengoptimalkan jumlah data yang harus disimpan, maka dimungkinkan untuk melakukan monitoring parameter-parameter yang dianggap kritis dan penting, dan monitoring secara lebih rinci akan dilakukan jika dideteksi terjadi anomali pada kinerja sistem yang dimonitor, dengan menggunakan sistem monitoring yang dapat melakukan monitoring dari semua parameter yang tersebut di atas.

n. Untuk mengoptimalkan jumlah data yang harus disimpan, maka NMS akan melakukan akumulasi data kinerja tersebut secara harian, dimana setelah itu data rinci dapat dihapuskan. Interval waktu penghapusan data rinci ini akan ditetapkan secara prosedural oleh pihak IT.

Pemeliharaan *Database* oleh DBA (*Database Administrator*)

a. Untuk seluruh aplikasi operasional yang menggunakan *database*, DBA bertanggung jawab untuk memelihara sistem *database* tersebut.

b. DBA adalah satu-satunya pihak yang melakukan instalasi, konfigurasi, pengawasan dan pemeliharaan *database* yang digunakan di Danareksa, baik yang untuk kegiatan operasional maupun untuk kegiatan pengembangan.

c. DBA harus memastikan keamanan *database* yang dipeliharanya, sesuai dengan kebijakan Keamanan dan Keselamatan yang telah disetujui.
d. Secara periodik ISO akan melakukan pengamatan atas keamanan informasi yang tersimpan dalam *database* perusahaan, dan bekerja sama dengan DBA untuk menangani risiko-risiko yang terlihat selama pengamatan tersebut.
e. DBA juga harus melakukan *patching/hotfix* ke *database* yang dipeliharanya segera setelah *patching/hotfix* tersebut direkomendasikan oleh ISO, sehingga dianggap aman untuk *database* yang digunakan di Danareksa. Jeda waktu antara terbitnya rekomendasi untuk *patching/hotfix* ini dengan waktu instalasi atau implementasi di *database* Danareksa adalah maksimum satu bulan.
f. DBA bertugas untuk memastikan tercapainya kondisi optimum untuk operasional *database* dengan melakukan monitoring dan *tuning* secara kontinyu kinerja sistem *database* yang digunakan di Danareksa, antara lain atas keakuratan, kelengkapan dan kesahihan data (*accuracy*, *completeness and validity*) selama seluruh proses transaksi *database* terjadi. Monitoring secara periodik ini harus dilakukan dengan bantuan perangkat keras dan lunak pembantu atau melalui serangkaian *automatic scripts* yang akan memberikan notifikasi ke DBA jika terjadi kinerja yang tidak normal. Parameter yang harus dimonitor telah disebutkan di bagian X.7. Kebijakan. di atas.
g. Jika dari monitoring di atas terlihat kekurangan kinerja *database* maka DBA harus mengidentifikasikan sumber permasalahan yang mungkin. Jika ukuran *disk space* dirasa kurang, maka DBA harus mengusulkan *upgrade* yang diperlukan, dilengkapi dengan rencana implementasi kepada IT Service Delivery. Jika disebabkan oleh kurangnya spesifikasi server yang digunakan, maka DBA harus mengusulkan *upgrade* yang diperlukan kepada IT Service Delivery. Pada kedua kasus di atas usulan ini harus disetujui oleh Kepala Divisi IT dengan persetujuan Direksi dimana perlu. Dalam hal ini DBA akan bekerja sama dengan administrator sistem dan perangkat keras yang terkait.
h. DBA harus melakukan penyelesaian masalah yang timbul dan dilaporkan oleh pengguna *database* dan aplikasinya. DBA harus melakukan penjadwalan - kegiatan yang dapat dilakukan secara otomatis ataupun dengan *script* untuk mengoptimalkan sumber daya sistem yang ada.
i. Pertukaran data dari sistem operasional ke sistem pengembangan harus dilakukan oleh DBA. Jika sistem pengembangan dikelola oleh pihak ketiga atau eksternal, maka jika ada informasi yang sifatnya rahasia pada data yang diminta, DBA harus melakukan sanitasi (membuang atau mengganti bagian data yang sifatnya rahasia) sebelum memberikan data tersebut untuk di-*install* di sistem *database* pengembangan.
j. Migrasi data kedalam sistem *database* operasional harus dilakukan oleh DBA, dan dengan menimbulkan gangguan sekecil-kecilnya pada sistem operasional tersebut. DBA akan memberikan terlebih dahulu jadwal implementasi dari migrasi ini, dan harus disetujui oleh kepala unit kerja IT dan kepala unit kerja unit kerja pengguna utama aplikasi *database* tersebut.

k. Kegiatan *support* atau *tuning* yang mengakibatkan perubahan data seperti perubahan desain *database*, atau juga "archiving," "purging," dan "pruning" harus dilakukan DBA dengan sebelumnya memberikan rencana implementasi yang harus disetujui oleh Kepala Divisi IT dan Kepala Divisi pengguna utama aplikasi *database* tersebut. Sebelum semua kegiatan di atas harus dilakukan *backup* lengkap terhadap *database* dimana kegiatan tersebut di atas dilakukan.

l. DBA harus melakukan pemeriksaan secara rutin terhadap *log* yang dihasilkan oleh sistem *database*, termasuk *log* untuk transaksi, *error* dan *event* lain yang terjadi dan tercatat.

m. DBA harus melakukan kegiatan *backup database* menurut jadwal yang telah ditentukan. *Backup* yang dilakukan ini termasuk *backup* skema dan konfigurasi *database*, serta informasi lainnya yang diperlukan untuk instalasi dan operasional sistem *database*. Hasil *backup database* tersebut disimpan di satu lokasi *hard disk* yang telah ditentukan, untuk kemudian di-*backup* ke *tape* oleh personel IT Service Delivery. Jika ada *restore* yang perlu dilakukan dari *tape*, maka DBA akan meminta IT Service Delivery untuk melakukan *restore data* yang diperlukan ke lokasi *hard disk* tersebut, untuk kemudian DBA melakukan *restore database*.

n. DBA harus melakukan *testing restore database* yang di-*backup*-nya, minimal satu bulan sekali. Jika ditemukan kegagalan *restore*, maka hal ini harus dilaporkan ke kepala unit kerja IT untuk kemudian ditindaklanjuti, terutama mengenai hasil backup setelah testing terakhir kali yang berhasil sampai terjadinya kegagalan tersebut.

o. DBA harus melakukan kontrol akses berdasarkan *database* aplikasi yang ada, dan berdasarkan permintaan dari pengguna langsung secara formal dan tercatat, yang disetujui oleh Kepala Divisi yang bersangkutan, dan Kepala Divisi pengguna utama *database* dan aplikasi tersebut, jika ada. DBA dapat menetapkan suatu "proxy' administrator akses yang akan diberikan delegasi untuk menetapkan daftar akses untuk database suatu aplikasi tertentu. Proses penunjukkan "proxy" ini harus dilakukan secara tercatat dan formal, dengan persetujuan Kepala Divisi IT.

p. Semua kegiatan di atas harus dilakukan secara formal dan tercatat, dengan berita acara yang ditandatangani oleh semua pihak yang terkait dan terlibat.

XI. MANAJEMEN KUALITAS LAYANAN TEKNOLOGI INFORMASI

XI.1. Monitor dan Evaluasi Kinerja TI

Tujuan

Kebijakan ini bertujuan untuk memastikan bahwa seluruh kinerja TI sesuai dengan arahan dan kebijakan yang berlaku.

Ruang Lingkup

Kebijakan ini meliputi pengaturan pendekatan dan metoda monitoring kinerja TI, pendefinisian dan cara pengumpulan data, proses asesmen kinerja TI, proses pelaporan kinerja TI secara periodik, dan proses perencanaan remediasi akibat deviasi hasil asesmen kinerja TI.

Deliverable

Implementasi kebijakan ini dapat dituangkan dalam prosedur pengukuran kinerja yang didefinisikan dalam *Key Performance Indikator* (KPI) unit, prosedur tata cara pengumpulan data kinerja TI, prosedur proses pelaksanaan asesmen kinerja TI, prosedur pelaporan kinerja TI, dan prosedur tata cara remediasi deviasi kinerja TI.

XI.2. Monitor dan Evaluasi Pengendalian Internal

Tujuan

Untuk memberikan jaminan mengenai operasi TI yang efektif dan efisien dan kepatuhannya terhadap kebijakan dan aturan yang berlaku.

Ruang Lingkup

Kebijakan ini mengatur proses monitoring dan pelaporan pengecualian pengendalian (*control exception*), pengelolaan asesmen dan hasil dari *Control Self Assessment* (CSA), mengelola proses remediasi, dan *review* pihak ketiga.

Kebijakan

Implementasi Kebijakan ini dapat dituangkan dalam pendefinisian pengendalian internal yang akan diterapkan dalam layanan TI, prosedur pelaporan pengecualian kontrol, prosedur asesmen dan CSA, prosedur tata cara remediasi, dan prosedur tata cara mengevaluasi pihak ketiga.

XI.3. Pengelolaan *Compliance External Regulation*

Tujuan

Kebijakan ini bertujuan untuk memastikan bahwa persyaratan aturan atau hukum yang berlaku telah dipatuhi.

Ruang Lingkup

Kebijakan ini mengatur proses identifikasi persyaratan *compliance*, mengoptimalkan dan mengevaluasi tanggapan terhadap hasil audit, memastikan tingkat kepatuhan, dan menyusun laporan yang terintegrasi dengan bisnis.

Kebijakan

Implementasi kebijakan ini dapat dituangkan dalam pendefinisian kebutuhan persyaratan *compliance* terhadap aturan tertentu (misal Sarbanes-Oxley, Basel II, PCI, Peraturan Bank Indonesia no.9/15/PB1/2007, prosedur pengelolaan *review* terhadap audit eksternal dan prosedur penyusunan laporan yang terintegrasi dengan laporan bisnis.

XI.4. Standar Kualitas Layanan dan Pelaporan

Tujuan

Membentuk suatu standar kualitas layanan (*Service Quality Standard*), beserta mekanisme pelaporan dan monitoring-nya yang akan digunakan sebagai acuan untuk layanan yang diberikan oleh Divisi IT kepada semua *User* di Danareksa.

Ruang Lingkup

Seluruh layanan yang diberikan secara rutin dan operasional oleh pihak IT kepada *user*, balk dilakukan sendiri atau dengan melibatkan pihak ketiga.

Tanggung Jawab

a. Pihak IT akan memberikan layanannya sesuai dengan standar kualitas yang telah ditetapkan dalam kebijakan ini.
b. Jika layanan dilakukan oleh pihak ketiga, maka pihak ketiga tersebut wajib memastikan bahwa tingkat kualitas layanannya akan sama atau lebih baik daripada standar tingkat kualitas yang ditetapkan oleh kebijakan ini, dan juga untuk melakukan kegiatan pelaporan periodik seperti yang telah dijanjikan.
c. Pihak IT melakukan pengawasan atas layanan pihak ketiga, terutama dalam kaitan pelaporan dan review, sebagai wakil dari pihak internal Danareksa. Untuk layanan yang bersifat "back-to-back'" pihak IT ikut terlibat dalam kegiatan pelaporan dan review bersama dengan pihak internal Danareksa.
d. *User* layanan tersebut wajib bersikap proaktif dan memberikan pemberitahuan ke IT jika dirasakan bahwa layanan tidak memenuhi standar yang telah ditetapkan.

Kebijakan

a. Jenis layanan yang diberikan oleh IT kepada *user* Danareksa dibagi menjadi beberapa kategori, dan masing-masing mempunyai standar kualitas layanan-nya sendiri.
b. Jenis layanan di atas dikategorikan sebagai berikut:
   i. Layanan *Helpdesk*: pemeliharaan dan perawatan perangkat keras dan perangkat lunak standar perangkat komputer, diantaranya adalah sebagai berikut:
      1. Penyelesaian dari permasalahan yang ada (*troubleshooting problems*);
      2. Pendukung aktivitas produksi (*production support*);
      3. Manajemen infrastruktur (*infrastructure management*).

   ii. Layanan ketersediaan data yang dilakukan oleh IT Service Delivery: *file*, dan *print server*, *backup* dan *recovery*.

   iii. Layanan jaringan dan komunikasi data yang dilakukan oleh IT Service Delivery, diantaranya adalah sebagai berikut:
      1. Mengelola dan memelihara kinerja infrastruktur;
      2. Penyelesaian masalah dari kesalahan yang ada (*troubleshooting errors*);
      3. Memelihara database (*maintaining databases*);
      4. Mencadangkan dan memulihkan layanan (*backing up & restore services*);
      5. Memantau aktifitas infrastruktur IT;
      6. Melakukan analisis *downtime*;
      7. Menyusun laporan apabila terjadi kegagalan sistem dan implikasi dari hal tersebut.

   iv. Administrasi aplikasi: *update*, *upgrade* dan pemeliharaan, diantaranya adalah sebagai berikut:
      1. *Software Maintenance*
         Adanya rekomendasi terhadap pengembangan aplikasi, baik selama pemeliharaan aplikasi yang ada dan sewaktu proses *upgrade* aplikasi.
      2. *Production Support*
         Mendukung kegiatan produksi berupa perbaikan diantaranya memperbaiki kesalahan (*fix error*) dan perbaikan terhadap interupsi yang terjadi pada sistem yang sudah berjalan (yaitu, aplikasi, *mainframe* dan database) yang berada pada area produksi.
         Penyedia layanan perlu menyelidiki penyebab kesalahan dan interupsi yang terjadi serta segera melakukan perbaikan terhadap masalah tersebut dengan cepat.

Waktu yang digunakan untuk penyelesaian masalah (*problem solving*) tersebut harus lebih cepat daripada proses pemeliharaan (*maintain*), karena sistem produksi digunakan dalam proses bisnis sehingga organisasi dapat segera menggunakan system tersebut.

v. Administrasi dan pengolahan data oleh DCO, diantaranya adalah sebagai berikut:
   1. *Hardware*, *software*, dan perencanaan sistem operasi (*operating system*), termasuk: spesifikasi, pengadaan, instalasi, konfigurasi, pemeliharaan, *upgrade*, dan pengelolaan;
   2. Pemantauan terus menerus dari kinerja *server* dan status operasional;
   3. Manajemen kapasitas *server*, termasuk perencanaan kapasitas, *load balancing*, *tuning*, dan konfigurasi ulang;
   4. Instalasi aplikasi *software server* dan *upgrade* sesuai rilis yang disepakati oleh *User* dan penyedia layanan;
   5. Instalasi dari sistem yang sedang berjalan dan manajemen *hardware* dan *software*;
   6. Administrasi keamanan dan melakukan *backup data* untuk memastikan keamanan dan integritas sistem dan aplikasi;

   Pemulihan sistem *server* dalam hal terjadi bencana dengan mengikuti standar yang ditetapkan.

vi. Pengadaan perangkat komputer dan teknologi, bekerja sama dengan Unit Kerja Procurement atau General Affair.

vii. Layanan manajemen jasa sekuriti (*managed security services*): layanan yang memantau keamanan organisasi IT, diantaranya adalah sebagai berikut:
   1. Keseluruhan infrastruktur IT
   2. *Asset data*;
   3. Manajemen aktivitas dari pengguna layanan.

c. Untuk beberapa layanan yang tercakup dalam jenis layanan di atas, pihak IT dapat membuat suatu SLS atau SLA yang akan menyatakan suatu acuan tingkat kualitas layanan yang akan diberikannya, Pemilihan penggunaan SLS atau SLA harus diambil sesuai dengan definisi masing-masing yang telah dijabarkan di atas.
d. Untuk layanan-layanan TT yang termasuk dalam kategori "critical' atau sangat penting, harus dibuat SLS atau SLA-nya masing-masing. Pemberian kategori ini harus didasarkan pada kebijakan Manajemen Ketersediaan Layanan

(*Contingency Management*) yang diatur secara terpisah, dan disetujui oleh pihak Manajemen Danareksa.

e. Untuk semua jenis layanan di atas, harus diidentifikasikan secara jelas user dari layanan, yang dapat berupa seluruh pengguna komputer di Danareksa, atau suatu kelompok yang merupakan *subset* daripadanya.
f. Sebagai acuan tingkat kualitas layanan di atas, baik pada SLS maupun SLA, harus diambil parameter dari daftar di bawah ini sebagai tolok ukur kinerja layanan IT, antara lain:
   i. ***Uptime/Availability***: memberikan ukuran ketersediaan yang dihitung dari total waktu layanan tersebut tersedia dibandingkan dengan total waktu.
   ii. ***Response time***: dihitung dari waktu pertama kali user melakukan kontak ke Helpdesk untuk kebutuhan suatu layanan sampai dengan waktu layanan tersebut didapatkan (*response time*).
   iii. ***Resolution time***: yang menggambarkan jangka waktu user melakukan kontak dengan *Helpdesk* sampai dengan masalah tersebut diselesaikan. Jangka waktu satu layanan berada dalam status Pending, misalnya karena membutuhkan informasi tambahan dari user atau layanan tambahan dari pihak lainnya, tidak akan dihitung dalam response time ataupun *resolution time*.
   iv. **Closure ratio**: perbandingan dari jumlah permintaan bantuan ke Helpdesk yang berhasil diselesaikan, dibandingkan dengan total jumlah permintaan. Dapat juga ditambahkan dengan *closure-non-pending ratio*, dimana jumlah tiket yang belum selesai karena berada dalam status Pending, tidak dimasukkan dalam perhitungan statistik ini,
   v. ***Service Delivery Ratio***: perbandingan antara proses yang terlaksana secaraakurat dan tepat waktu dibandingkan dengan layanan yang diminta.
g. Untuk setiap parameter yang dipilih dari di atas akan diberikan suatu angka target kualitas layanan yang harus dipenuhi. SLS atau SLA yang telah ditetapkan, lengkap dengan parameternya dan angka targetnya, harus disetujui oleh Kepala Divisi IT dan Direksi. Khusus untuk SLA, parameter dan targetnya harus juga disetujui oleh semua user layanan terkait.
h. Parameter kualitas layanan dan angka targetnya masing-masing akan menjadi dasar dari proses monitoring, pelaporan dan review untuk SLS dan SLA tersebut.
i. Dokumen SLS/SLA paling tidak harus memuat komponen dasar sebagai berikut:
   i. **Tujuan dan pihak-pihak yang terlibat** yang akan menjelaskan batasan--batasan yang dimiliki oleh dokumen SLS/SLA tersebut, termasuk
   ii. **Kondisi dan persyaratan awal** yang harus dipenuhi oleh semua pihak agar SLS/SLA ini dapat diberlakukan secara penuh, yang pada dasarnya merupakan daftar hak dan kewajiban semua pihak yang terlibat, dan
   iii. **Detail serta lingkup layanan dan kegiatan** yang tercakup dalam dokumen SLS/SLA yang disetujui. Jam operasional, daftar layanan, daftar target user dan sistem atau aplikasi termasuk hak dan kewajiban setiap pihak dimana standar kualitas layanan ini akan berlaku harus dicantumkan pada bagian

iv. **Pengecualian** yang dapat diberlakukan untuk layanan yang tercakup, jika satu dan lain kondisi yang dipersyaratkan tidak dapat dipenuhi, termasuk proses untuk melakukan pengecualian tersebut.
v. **Daftar kontak** dari masing-masing pihak yang terkait. Segala proses dan prosedur yang berhubungan dengan SLS/SLA ini akan dilakukan oleh kontak yang telah ditunjuk dalam daftar.
vi. **Parameter** yang digunakan untuk pengukuran kinerja.
vii. **Mekanisme monitoring** berupa tatacara atau perangkat yang digunakan untuk mengukur parameter yang telah ditetapkan.
viii. **Pelaporan kinerja** yang akan dilakukan oleh pihak IT.
ix. **Proses review** laporan dan keseluruhan tingkat kualitas layanan yang sudah disetujui.
x. **Metode pengaduan dan klarifikasi** yang mungkin terjadi dalam proses review di atas.
xi. **Bagian persetujuan** dari semua pihak yang terlibat dalam pemberian layanan termaksud, dengan persetujuan akhir dari Kepala Divisi IT dan Direksi Penanggungjawab IT.

j. Semua komponen dan isi SLS/SLA harus sesuai dengan peraturan dan perundangan yang berlaku.
k. Untuk setiap SLS/SLA yang telah ditetapkan, secara periodik minimal setahun sekali harus dilakukan survey kepuasan *User*, untuk mendapatkan umpan baik mengenai layanan yang tercantum dalam SLS/SLA tersebut.

Monitoring, Pelaporan dan Review

a. Setiap dokumen SLS/SLA yang resmi berlaku harus mencantumkan tata cara pelaporan periodik dan review kinerja.
b. Selain melalui pelaporan, setiap pihak yang terlibat, termasuk user internal Danareksa, harus bersikap proaktif serta melakukan monitoring dan koordinasi langsung untuk menjaga kualitas layanan dalam tingkatan yang telah disetujui.
c. Untuk keperluan monitoring ini, terutama untuk layanan yang langsung dilakukan oleh IT, pihak IT dapat menyediakan sistem tampilan data kumulatif tingkat kualitas layanan yang telah diberikan, untuk diakses atau diterima oleh semua pihak terkait.
d. Jika karena satu dan lain hal terjadi gangguan yang menyebabkan standar kualitas ini tidak akan dapat dipenuhi, maka pihak pemberi layanan wajib mengirimkan eksepsi dalam bentuk pemberitahuan tertulis kepada semua *User* layanan tersebut paling lambat 5 (lima) hari dimuka.
e. Setiap dokumen SLS/SLA yang resmi berlaku harus mencantumkan tatacara klarifikasi hasil laporan. Tatacara ini mengatur jika terjadi perbedaan data antara pemberi dan penerima layanan mengenai tingkat kualitas layanan, sehingga diperlukan kiarifikasi.
f. Proses klarifikasi ini harus dapat diselesaikan oleh semua pihak yang terlibat dalam waktu 14 (empatbelas) hari kerja.

XI.5. Manajemen Tingkat Kualitas Layanan

Tujuan

Mengatur dan memonitor semua layanan yang disediakan oleh IT, baik yang dilakukan oleh pihak internal ataupun oleh pihak ketiga, yang sudah resmi SLS/SLA nya, serta mengatur proses pencapaian tingkat layanan yang telah ditetapkan serta pengembangan dan perbaikannya.

Ruang Lingkup

Semua kontrak penyediaan layanan, baik internal ataupun eksternal, yang melibatkan IT, dan sudah resmi menggunakan SLS/SLA.

Tanggung Jawab

Pihak IT harus memastikan semua layanan IT yang diberikannya, termasuk yang dilakukan oleh pihak ketiga, minimum memenuhi batas tingkat kualitas yang ditentukan.

Kebijakan

a. Pihak IT memastikan bahwa layanan yang diberikan sudah sesuai dengan kebutuhan pengguna layanan baik secara fungsional maupun non fungsional dan memastikan standar kualitas layanan secara umum yang meliputi kinerja, kapasitas dan keamanan layanan.
b. Pihak IT harus melakukan pengaturan dan pengawasan untuk memastikan bahwa layanan IT yang disediakannya memiliki kinerja sesuai dengan yang dijanjikan, dan berada pada batas parameter yang ditentukan dalam SLS/SLA layanan yang terkait.
c. Pihak IT dapat menggunakan teknologi seperti situs web intranet untuk melakukan konsolidasi atas laporan kualitas layanan yang diterima dan dikirimkannya, untuk dapat diakses secara cepat oleh *User* dan pihak-pihak terkait lainnya.
d. Pihak IT harus memastikan bahwa kinerja layanannya telah berlangsung dengan optimal. Untuk itu setiap tiga periode pelaporan dapat dilakukan review kinerja dengan pihak *User* dan pihak terkait lainnya.
e. Pihak IT dapat menggunakan teknologi untuk melakukan notifikasi atau alert bilamana terjadi tingkat kualitas layanan yang berada dibawah tingkat SLS/SLA yang telah ditetapkan. Sistem notifikasi atau *alert* yang digunakan harus mempunyai suatu hierarki eskalasi sesuai dengan tingkat gap yang terjadi.

f. Jika selama periode review tertentu berturut-turut dicapai tingkat kualitas melebihi SLS/SLA yang telah ditetapkan, maka dapat diusulkan untuk diadakan perbaikan atau peningkatan parameter tersebut, yang harus disetujui oleh semua pihak yang terlibat. Tata cara dan prosedur untuk peningkatan tingkat kualitas ini akan ditentukan kemudian.
g. Jika target tingkat kualitas tidak tercapai dalam dua periode pelaporan secara berturut-turut dalam satu periode review, maka saat review harus dibuat suatu rencana kerja atau perubahan proses dengan sasaran untuk perbaikan layanan yang diberikan dan pencapaian tingkat SLS/SLA yang telah ditetapkan. Rencana kerja atau perubahan proses ini harus disetujui oleh semua pihak yang terlibat, *User* dan pihak IT.

h. Jika target tingkat kualitas tidak tercapai secara berturut-turut dalam dua periode review, maka harus dilakukan review menyeluruh dimana seluruh unit kerja terkait terwakili, bersama dengan Direksi Penanggungjawab IT, dan ditetapkan rencana perubahan menyeluruh, yang dapat melibatkan perubahan pada parameter yang telah ditetapkan.

XI.6. Manajemen Tingkat Kualitas Operasional

Tujuan

Mengatur kerja sama antar bagian internal IT, dan untuk koordinasi yang memungkinkan tercapainya tingkat kualitas layanan yang dikehendaki untuk semua layanan yang disediakan oleh IT.

Ruang Lingkup

Semua layanan yang diberikan oleh IT, baik internal ataupun eksternal, yang melibatkan IT, dan terutama yang sudah resmi menggunakan SLS/SLA.

Tanggung Jawab

Semua pihak internal IT harus memastikan komitmen dan kerjasamanya dalam menjaga layanan IT kepada pihak lain di Danareksa agar minimum memenuhi batas tingkat kualitas yang telah ditentukan.

Kebijakan

a. Untuk setiap SLS/SLA yang ditetapkan oleh IT dan sudah resmi berlaku, jika layanan tersebut dilakukan atau dicapai oleh lebih dari satu bagian atau pihak di IT, maka harus dibentuk suatu *Operational Level Agreement* (OLA) yang mengikuti bentuk SLS/SLA tersebut.

b. Untuk layanan TI lainnya yang tidak terdapat SLS/SLA, maka pihak IT tetap dapat merumuskan suatu OLA jika layanan tersebut dilakukan oleh lebih dari satu bagian atau pihak di dalam IT.
c. Untuk setiap SLS/SLA yang ditetapkan oleh IT dan sudah resmi berlaku, jika layanan tersebut dilakukan atau dicapai dengan kerjasama antara pihak IT dan pihak ketiga, maka IT harus membentuk OLA untuk bagian layanan tersebut, dan memastikan bahvva OLA tersebut dipenuhi oleh bagian-bagian operasional IT.
d. Penanggungjawab SLS/SLA yang telah resmi berlaku harus melakukan koordinasi dengan penanggung jawab dari OLA yang menjadi bagian SLS/SLA tersebut. Pada setiap saat harus dapat diketahui kinerja dan masing-masing bagian yang menyediakan layanan tersebut.
e. Harus diusahakan batasan yang jelas untuk masing-masing OLA, sehingga *overlap* dan duplikasi antara OLA dapat diminimalkan.

XII. MANAJEMEN KELANGSUNGAN USAHA

XII.1. Manajemen Kelangsungan Usaha

Tujuan

Membuat suatu kerangka dan aturan dalam memastikan bahwa seluruh proses dan kegiatan operasional penting perusahaan dapat dijaga kelangsungannya secara efektif dan efisien dalam keadaan darurat untuk meminimalkan dampak dan konsekuensi finansial, legal, reputasi dan lain-lain.

Ruang Lingkup

Seluruh layanan yang diberikan kepada nasabah Danareksa, termasuk seluruh komponen pendukung yang diperlukan untuk memberikan layanan tersebut

Tanggung Jawab

a. Pihak Direksi dan Kepala Unit Kerja untuk menempatkan manajemen kelangsungan usaha ini sebagai bagian integral dari kegiatan operasionalnya sehari-hari, dan bagian dari manajemen pengelolaan risiko secara umum.
b. Unit Kerja Risk Management untuk melakukan konsolidasi dan pembaharuan secara periodik rencana kegiatan operasional Danareksa dalam keadaan darurat, yang hendak diimplementasikan oleh seluruh unit kerja di Danareksa. Dokumen konsolidasi rencana seluruh unit kerja ini membentuk BCP Danareksa.
c. Pihak IT untuk melihat potensi gangguan terhadap layanan Danareksa yang berbasiskan IT dan teknologi, dan membuat suatu rencana kesiapan penanggulanggannya.
d. Seluruh pihak Danareksa yang terlibat dalam BCM ini secara operasional untuk melakukan *testing* secara periodik rencana kelangsungan operasional dalam

keadaan darurat (*Business Continuity Plan* atau BCP) untuk memastikan bahwa rencana tersebut masih *up-to-date* dan layak untuk dilakukan

Tugas dan Tanggung Jawab *Incident Management Team* (IMT)

a. Tugas utama IMT adalah untuk memutuskan dimulai dan selesai berlakunya keadaan darurat, serta tingkatan keadaan darurat yang terjadi. Proses dan prosedur penetapan keadaan darurat tersebut akan diatur secara tersendiri.
b. Untuk menentukan tingkat siaga yang akan ditetapkan, IMT harus terlebih dahulu melakukan analisa gangguan (*damage assessment*). IMT harus secepat mungkin mendapatkan fakta-fakta kejadian penyebab, dan terutama mengenai tingkat kerusakan atau gangguan yang sudah dan potensial akan terjadi, lamanya gangguan dan klasifikasi informasi yang terganggu. Dari hasil analisa ini, IMT menetapkan tingkat siaga keadaan darurat yang terjadi, dan mengaktifkan seluruh proses dan prosedur yang berkenaan dengan operasional dalam keadaan darurat (BCP),
c. IMT memelihara suatu pohon komunikasi (*communication tree*) yang menetapkan secara jelas nomor kontak untuk setiap unit kerja yang terlibat dalam BCP. Pohon komunikasi ini harus dijaga dan langsung diperbaharui setiap terjadi perubahan, untuk dikomunikasikan kembali ke seluruh pihak yang terlibat dalam keadaan darurat.
d. IMT membantu Unit Compliance dalam memastikan bahwa setiap unit kerja Danareksa telah melaksanakan proses yang ditetapkan di atas dengan hasil suatu BCP yang realistis dan siap untuk dilaksanakan.
e. IMT bersama dengan Unit Kerja Risk Management melakukan konsolidasi seluruh BCP unit kerja Danareksa, dan membentuk suatu BCP Danareksa.
f. IMT menetapkan bahwa seluruh fungsi dan fasilitas pendukung yang dibutuhkan selama keadaan darurat terjadi, telah tersedia secara cukup dan operasional. IMT dapat melakukan penugasan yang diperlukan kepada unit kerja yang sesuai dengan fungsi dan fasilitas yang diperlukan.
g. IMT harus memastikan bahwa BCP Danareksa telah sesuai dengan tingkat keperluan internal maupun eksternal untuk mendukung tujuan Kebijakan di atas, dan telah sesuai dengan seluruh peraturan dan perundangan yang berlaku untuk semua kantor dan lokasi operasional Danareksa.
h. IMT melakukan koordinasi dengan seluruh Unit Kerja Danareksa yang melakukan operasionalnya dalam keadaan darurat tersebut, dan memastikan bahwa layanan yang diberikan Danareksa dalam keadaan darurat tersebut sesuai dengan standar SLA/SLS yang berlaku. IMT memastikan bahwa seluruh pihak internal ataupun pihak ketiga yang memberikan dukungan telah memenuhi SLA/SLS-nya.
i. IMT harus memastikan bahwa sumber gangguan terus diupayakan untuk diatasi sejauh dimungkinkan secara internal. Jika sumber gangguan berasal dari eksternal Danareksa, maka Danareksa juga harus membantu sejauh dalam kewenangannya untuk mengatasi gangguan tersebut.

j. Selama dalam keadaan darurat ini, IMT berhak untuk melakukan pengecualian atas kebijakan yang berlaku internal dalam kondisi normal, untuk memenuhi standar layanan dan SLA/SLS nya.
k. IMT harus memastikan bahwa semua pengecualian ini, dan ketidaksempurnaan atau potensi perbaikan BCP yang ada, akan dicatat dan dikonsolidasikan. Konsolidasi catatan ini akan dipergunakan pada sesi review berikutnya dari BCP tersebut.
l. IMT bekerja sama dengan pihak internal ataupun instansi eksternal terkait, dan terus memantau keadaan darurat yang terjadi, serta meneruskan komunikasinya sesuai kebutuhan seluruh pihak yang terlibat, Pada saat keadaan darurat ini, berdasarkan informasi yang terus diterimanya, IMT dapat melakukan perubahan tingkat siaga yang terjadi, memperluas atau mempersempit lingkup keadaan darurat, ataupun menentukan bahwa keadaan darurat telah berakhir.
m. Jika keadaan darurat telah dinyatakan berakhir, maka IMT juga melakukan koordinasi dalam masa transisi dari operasional masa darurat kembali ke keadaan operasional normal. Hal ini juga merupakan lingkup dari dokumen BCP yang berlaku di Danareksa. IMT harus memastikan bahwa masa transisi ini berlaku sesingkat mungkin, dimana secara bertahap layanan Danareksa yang dilakukan dari proses darurat dikembalikan ke proses normalnya.
n. Setelah proses terakhir selesai dikembalikan ke proses normalnya, maka IMT dapat menyatakan secara resmi bahwa keadaan darurat tidak berlaku lagi.
o. Di akhir setiap proses keadaan darurat IMT melakukan sesi diskusi (*debrief*) untuk melakukan penilaian secara umum pelaksanaan BCP Danareksa. Untuk sesi tersebut IMT harus mengundang seluruh unit kerja dan pihak yang terlibat selama keadaan darurat, dimana paling tidak 60% dari undangan hadir atau terwakili dalam sesi diskusi tersebut. Pada sesi diskusi ini dapat dipersiapkan masukan untuk penyempurnaan BCP Danareksa berdasarkan catatan yang dilakukan saat keadaan darurat.
p. IMT harus memastikan bahwa setiap unit kerja memelihara BCP-nya masing-masing agar tetap valid dan realists. IMT harus memastikan bahwa BCP Danareksa secara keseluruhan tetap valid dan realistis. Diluar keadaan darurat, IMT harus secara periodik melakukan *testing* atas BCP yang berlaku, baik secara *walk-through*, secara *table-top*, ataupun dengan cara lain yang dianggap dapat mewakili. Dalam satu tahun BCP tersebut harus diaplikasikan paling tidak satu kali, baik melalui keadaan darurat yang sebenarnya, ataupun melalui *testing*.

Kebijakan

a. Danareksa menentukan suatu standar kualitas layanan (SLA/SLS/SLG) yang akan menentukan tingkat toleransi Danareksa terhadap gangguan atas layanan yang terjadi. Pertimbangan untuk standar kualitas ini juga harus memperhatikan faktor non-teknis seperti reputasi, tanggungjawab secara legal, finansial, sosial politik ataupun faktor-faktor lainnya yang dirasa perlu.

b. Untuk memenuhi tujuan pada huruf (a) tersebut, Danareksa melakukan suatu manajemen kelangsungan usaha, dan membentuk suatu kesiapan melakukan kegiatan operasional dalam keadaan darurat.
c. Tingkatan kesiapan melakukan kegiatan operasional dalam keadaan darurat harus disesuaikan dengan kategori dasar keadaan darurat yang telah didefinisikan di atas.
d. Kondisi Siaga III dan Siaga II dapat diberlakukan untuk satu atau lebih kantor atau lokasi operasional Danareksa saja. Pada kondisi ini kinerja kantor atau lokasi operasional Danareksa lainnya tidak terganggu. Untuk kondisi Siaga I harus diberlakukan untuk seluruh kantor atau lokasi operasional Danareksa, dengan asumsi bahwa kegiatan operasional di kantor pusat mengalami gangguan layanan secara signifikan,
e. Danareksa membentuk suatu kelompok manajemen keadaan darurat yang disebut dengan *Incident Management Team* (IMT), yang minimal akan beranggotakan Direksi Danareksa, dengan dibantu keanggotaan lainnya. Hak dan tanggung jawab IMT telah diatur secara tersendiri di bagian berikutnya dalam kebijakan ini.
f. IMT menggantikan kelompok sejenis untuk pengendalian operasi keadaan darurat lainnya yang ada di Danareksa. Dengan dibentuknya IMT, maka kelompok-kelompok tersebut dinyatakan tidak beroperasi lagi.
g. IMT merupakan pusat koordinasi operasional Danareksa dalam keadaan darurat, dan menetapkan dimulai dan diakhirinya keadaan darurat, serta mengatur faktor-faktor operasional selama masa tersebut, termasuk dalam masa transisi untuk kembali ke kondisi operasional normal.
h. Koordinasi serta komunikasi saat keadaan darurat dipimpin oleh IMT.
i. Manajemen kelangsungan usaha akan mencakup langkah-langkah di bawah ini, yang detailnya akan diberikan dalam sub-kebijakan sendiri.
    i. Penetapan proses dan layanan penting yang diberikan.
    ii. Evaluasi dan asesmen risiko operasional yang mungkin terjadi, termasuk toleransi atas gangguan yang terjadi, terutama untuk proses dan layanan penting tersebut.
    iii. Analisa dampak gangguan terhadap kegiatan operasional perusahaan (*Business Impact Analysis*).
    iv. Penetapan skenario pemulihan kegiatan usaha dalam keadaan darurat, termasuk personil dan pihak yang terlibat di dalamnya.
    v. Penetapan rencana kelangsungan usaha (*Business Continuity Plan*).
    vi. Kegiatan *review* dan *testing*.
j. Setiap unit kerja harus memiliki rencana kelangsungan usaha (BCP) ini secara spesifik dan melaporkannya kepada IMT dan Unit Kerja Risk Management untuk dikonsolidasikan sebagai bagian dari rencana keseluruhan Danareksa. Setiap unit kerja harus mengetahui, sadar dan mengerti peran sertanya dalam BCP keseluruhan tersebut.

k. Pada BCP, baik spesifik maupun untuk keseluruhan Danareksa, harus dilakukan review dan pembaharuan secara periodik, minimal setiap dua tahun sekali. Dalam kegiatan review ini dapat juga dilakukan *testing* terhadap rencana BCP yang telah disepakati.

XII.2. Analisa Dampak Gangguan Terhadap Kelangsungan Usaha

Tujuan

Membuat analisa potensi gangguan dan dampaknya pada kelangsungan usaha, untuk membentuk suatu standar toleransi terhadap gangguan tersebut, serta melakukan segala persiapan operasional yang diperlukan. Dokumentasi dari analisa tersebut membentuk suatu *Business Impact Analysis* (BIA).

Ruang Lingkup

Seluruh layanan dan proses penting yang dilakukan oleh Unit Kerja Danareksa, yang secara langsung maupun tidak langsung diberikan kepada nasabah Danareksa.

Tanggung Jawab

a. Setiap unit kerja untuk menentukan seluruh layanan dan proses penting yang dilakukannya, dan menetapkan suatu standar pemberian layanan yang harus ditepatinya.
b. Unit kerja yang terlibat dalam kegiatan operasional Danareksa untuk melihat segala kemungkinan terhadap gangguan yang langsung berdampak terhadap kelangsungan usaha.

Kebijakan

a. Setiap unit kerja Danareksa harus mengidentifikasikan seluruh layanan dan proses penting yang dijalankannya dalam operasional sehari-Hari, yaitu yang mempunyai efek signifikan terhadap reputasi dan standar layanan nasabah jika terhenti selama berada dalam keadaan darurat.
b. Setiap Unit Kerja Danareksa harus menentukan semua potensi gangguan yang mungkin timbul dari setiap layanan dan proses penting yang telah diidentifikasikan pada huruf (a) di atas. Daftar gangguan tersebut bisa berasal dari alam (banjir, kebakaran clan gempa bumi), teknologi (kegagalan *hardware*, *software* atau listrik PLN), salah kornunikasi, atau sosial politik (huru hara ataupun demonstrasi). Dari daftar potensi dan probabilitas gangguan tersebut dapat dibuat analisa dampak dan kerugian yang dapat ditimbulkannya, baik secara finansial maupun non-finansial, *tangibles* (kerugian, kehilangan atau kerusakan benda atau perangkat) maupun intangibles (reputasi, keunggulan bersaing, atau kekayaan intelektual).

c. Dari hasil analisa tersebut, jika digabungkan dengan standar kualitas layanan yang telah ditentukan oleh Danareksa, dapat dibuat tingkat toleransi terhadap gangguan, baik dari sisi finansial maupun non-finansial, *tangibles* maupun *intangibles*. Toleransi ini dapat berbentuk waktu lamanya *downtime* yang diperbolehkan, ataupun penurunan tingkat kualitas layanan yang diperbolehkan.
d. Kumpulan dari informasi di atas membentuk suatu dokumen analisa dampak gangguan terhadap kelangsungan usaha Danareksa, atau suatu *Business Impact Analysis* (BIA), Laporan BIA tersebut harus menerangkan seberapa jauh dampak gangguan terhadap kegiatan operasional perusahaan sebelum batas toleransi yang ditentukan di atas mulai dilewati.
e. Danareksa harus memiliki analisa BIA ini untuk seluruh layanan dan proses penting yang telah ditentukan oleh unit kerja dan Manajemen Danareksa.
f. Unit Kerja Danareksa menggunakan hasil analisa BIA ini dalam mempersiapkan skenario atau rencana kelangsungan layanan dalam keadaan darurat yang mungkin diberlakukan, atau yang disebut *Business Continuity Plan* (BCP), yang akan diberikan secara lebih detil pada sub-kebijakan berikutnya.
g. Analisa BIA ini juga akan digunakan untuk menetapkan skala prioritas dari proses-proses penting di atas, dalam rangka kegiatan pemulihan layanan pada masa keadaan darurat.
h. Unit Kerja juga harus mempersiapkan daftar personil kunci yang harus ada dalam rangka melakukan layanan dan proses penting tersebut dalam keadaan darurat, dan untuk mempersiapkan kembalinya ke keadaan operasional normal jika keadaan darurat sudah selesai.
i. BIA pada tingkat Danareksa merupakan konsolidasi dari tingkat unit kerja, dan menjelaskan proses kunci dan proses pendukung yang akan dilakukan saat keadaan darurat, dan personil serta staf yang dibutuhkannya.
j. BIA pada tingkat Danareksa juga menjelaskan cara pencapaian layanan dalam keadaan darurat, serta fungsi dan fasilitas pendukung yang diperlukannya. Termasuk dalam rangka ini adalah pemilihan lokasi layanan darurat, atau *Disaster Recovery Site*.
k. Analisa dan pelaporan BIA ini harus dilakukan secara periodik, minimal setiap dua tahun sekali. Lingkup dari kegiatan analisa BIA di atas dapat dilakukan per satu unit kerja spesifik, ataupun sekaligus untuk seluruh Unit Kerja di Danareksa. Hasil akhir dari analisa BIA ini harus mencakup seluruh Unit Kerja di Danareksa.

XII.3. Rencana Kelangsungan Usaha Dalam Keadaan Darurat

Tujuan

Membuat suatu rencana pemberian layanan dan proses penting lainnya dalam keadaan darurat, agar tetap sesuai dengan standar kualitas layanan yang telah

ditentukan Danareksa. Dokumentasi dari rencana tersebut, lengkap dengan tujuan, lingkup, serta personil yang diperlukan membentuk suatu *Business Continuity Plan* (BCP).

Ruang Lingkup

Seluruh layanan dan proses penting yang telah diidentifikasikan oleh unit kerja dalam analisa BIA, dan merupakan layanan dan proses penting yang dijalankan untuk nasabah Danareksa, baik secara langsung ataupun yang tidak langsung.

Tanggung Jawab

a. Setiap Unit Kerja untuk menentukan rencana pemulihan seluruh layanan dan proses penting yang dilakukannya, dalam keadaan darurat.
b. Setiap Unit Kerja Danareksa untuk mempersiapkan semua fungsi dan fasilitas pendukung yang diperlukan untuk operasional dalam keadaan darurat.
c. Unit Kerja IT untuk membantu persiapan fungsi dan fasilitas pendukung di atas.

Kebijakan

a. Berdasarkan laporan BIA yang dilakukan, Unit Kerja harus mempersiapkan suatu rencana kelangsungan kegiatan yang telah dikategorikan sebagai layanan dan proses penting, dalam keadaan darurat. Rencana kelangsungan usaha ini akan membentuk suatu *Business Continuity Plan* (BCP) untuk Unit Kerja tersebut, dan secara konsolidasi membentuk BCP Danareksa secara umum.
b. BCP ini harus mencakup rencana yang telah disesuaikan dengan setiap kategori Siaga yang telah didefinisikan sebelumnya. BCP juga harus menjelaskan rencana yang bersifat umum, dan rencana yang hanya berlaku spesifik untuk suatu kategori siaga tertentu.
c. BCP harus dikondisikan untuk menjalankan layanan minimum yang diperlukan untuk mencapai standar kualitas layanan saat keadaan darurat, dan sedapat mungkin merupakan layanan lokal dengan biaya yang paling optimal. BCP juga harus dirancang untuk mampu secepatnya mencapai pemulihan layanan ke kondisi normal kembali, dengan tidak melupakan faktor kesehatan, keamanan dan keselamatan seluruh pegawai Danareksa dan personil lainnya yang terlibat.
d. Skenario pencapaian hal-hal tersebut di atas harus dibentuk secara terstruktur, prosedural, dan mengikuti suatu bentuk template yang akan ditetapkan tersendiri.
e. BCP juga harus mencakup kebutuhan personil, perangkat, fungsi dan fasilitas pendukung yang diperlukan untuk operasional dalam keadaan darurat. Untuk BCP konsolidasi Danareksa, maka Unit Kerja IT dan GA akan membantu mempersiapkan hal-hal yang terkait dengan teknologi dan premises secara

efektif, efisien dan terpadu. Jika dirasa perlu, Unit Kerja IT dan GA akan bekerja sama dengan pihak ketiga yang independen sebagai penyedia layanan yang diperlukan.

f. Untuk fasilitas pendukung yang bersifat tetap atau jangka panjang dan harus dipersiapkan sebelumnya, seperti lokasi *Disaster Recovery Center* (DRC), dan perangkat komputer yang dibutuhkannya, serta jaringan data yang diperlukan antar lokasi kantor, maka Unit Kerja IT akan mempersiapkannya berdasarkan kebutuhan kolektif unit-unit kerja di Danareksa, dan sedapat mungkin juga menggunakan lokasi atau fasilitas milik sendiri. Jika hal tersebut tidak dimungkinkan, maka dapat digunakan fasilitas atau layanan dari pihak ketiga yang independen.
g. Untuk setiap layanan pihak ketiga yang bersifat kontraktual, maka dalam kontraknya harus tercakup suatu standar kualitas layanan yang sesuai atau lebih baik dari standar kualitas layanan Danareksa pada keadaan darurat. Jika layanan ini juga digunakan pada keadaan operasional normal, maka standar kualitas layanan yang dijanjikan harus sesuai atau lebih baik dari standar kualitas layanan Danareksa pada keadaan normal.
h. Sebelum fasilitas pendukung yang bersifat tetap diatas tersedia, maka unit-unit kerja harus menetapkan BCP-nya masing-masing untuk dapat beroperasi tanpa fasilitas tersebut.
i. Penetapan BCP ini harus sesuai dengan dan memenuhi semua peraturan perundangan yang berlaku di kantor ataupun lokasi layanan Danareksa.
j. Dokumen BCP tersebut harus disimpan sehingga tidak ada kemungkinan kehilangan akses ke dokumen tersebut. Dokumen BCP harus secara aman di kantor ataupun lokasi operasional Danareksa, serta di lokasi di luar kantor yang dapat diakses secara mudah dan aman.
k. Paling tidak satu tahun sekali BCP tersebut harus diaplikasikan. Jika pada sepanjang tahun tidak stau kalipun dinyatakan keadaan darurat, maka harus dilakukan *testing* dalam bentuk *walk-through*, *table-top* ataupun bentuk lain yang dianggap tepat. Tujuan utama dari testing yang dilakukan adalah untuk memastikan bahwa setiap pihak tahu tugas dan kewajiban serta tanggungjawabnya masing-masing dalam operasional keadaan darurat.

XII.4. Rencana Pemulihan Layanan Teknologi dan Premises

Tujuan

Membuat suatu rencana persiapan pemberian layanan teknologi (IT) dan premises (GA) dalam keadaan darurat, agar tetap sesuai dengan standar kualitas layanan yang telah ditentukan Danareksa, dan rencana pemulihan layanan ke kondisi normalnya. Dokumentasi dari rencana tersebut secara lengkap akan membentuk suatu *Disaster Recovery Plan* (DRP) yang terutama mencakup layanan teknologi dan premises dari Unit Kerja IT.

Ruang Lingkup

Seluruh layanan yang berbasiskan teknologi dan premises, yang diberikan oleh Unit Kerja IT kepada Unit-unit Kerja lainnya di Danareksa, dan secara tidak langsung berupa layanan dan proses penting yang dijalankan untuk nasabah Danareksa. Contoh dari layanan tersebut misalnya, seluruh layanan komputer dan informasi elektronik, layanan komunikasi termasuk komunikasi seluler, fasilitas fisik untuk mendukung kegiatan layanan, serta layanan keamanan dan transportasi.

Tanggung Jawab

a. Setiap unit kerja untuk memberikan kepada Unit Kerja IT mengenai kebutuhan teknologi dan premisesnya dalam keadaan darurat.
b. Unit Kerja IT untuk melakukan konsolidasi kebutuhan tersebut, dan mempersiapkan fungsi dan fasilitas yang dibutuhkannya untuk seluruh unit kerja di Danareksa.

Kebijakan

a. Unit Kerja IT harus mempersiapkan fungsi dan fasilitas pendukung yang berbasiskan teknologi dan premises untuk memenuhi kebutuhan seperti yang dipaparkan dalam dokumen BIA dan/atau BCP baik untuk unit kerja tertentu, maupun untuk Danareksa secara keseluruhan.
b. Unit Kerja IT harus membuat dokumentasi BIA dan BCP-nya sendiri yang didalamnya tercakup fungsi dan fasilitas pendukung yang berbasiskan teknologi dan premises tersebut.
c. Unit Kerja IT harus menjaga keamanan dan keselamatan data, informasi serta fasilitas fisik, agar dapat digunakan dalam keadaan darurat sesuai dengan yang dibutuhkan. Hal pengamanan ini disesuaikan dengan cakupan dari Kebijakan Keamanan dan Keselamatan yang diatur tersendiri.
d. Unit Kerja IT harus tetap membina hubungan baik dengan penyedia layanan pihak ketiga, dan memastikan bahwa pihak ketiga tersebut sadar dan sanggup untuk memenuhi kebutuhan layanan dalam keadaan darurat, sesuai dengan yang dibutuhkan.
e. Rencana pemulihan pemberian layanan dalam keadaan darurat (DRP) ini harus mencakup setiap potensi kegagalan yang dianggap penting untuk jenis kegiatan operasional Danareksa, seperti bencana alam (banjir, kebakaran dan gempa bumi), kegagalan teknologi (dari *hardware*, *software* atau sumber daya listrik), atau konflik sosial politik (ancaman bom, huru hara ataupun demonstrasi).

f. DRP tersebut harus disesuaikan dengan ketiga kategori keadaan siaga yang telah didefinisikan di atas. Untuk kategori kegagalan parsial (Siaga III dan pada beberapa kasus Siaga II), maka pemulihan layanan sudah harus menjadi bagian dari proses kerja operasional sehari-hari dalam bentuk contingency plan. Untuk kategori kegagalan total, dengan rnengambil asumsi telah terjadi gangguan yang signifikan terhadap layanan teknologi dan premises, maka DRP akan mencakup penyediaan layanan pengganti.
g. Jika karena suatu sebab layanan pengganti tersebut tidak dapat disediakan oleh IT, maka hal ini harus diberitahukan kepada seluruh unit kerja sejak awal, dan semua unit kerja harus membuat suatu skenario operasional keadaan darurat dimana fasilitas pengganti tersebut tidak diperlukan.
h. Sebagai contoh dari huruf (g). di atas, jika IT belum dapat menyediakan lokasi pernulihan keadaan darurat atau *Disaster Recovery Center* (DRC), maka seluruh unit kerja harus membuat BIA/BCP nya dengan asumsi bahwa tidak ada DRC.
i. Pihak IT akan melakukan identifikasi layanan dan sistem utamanya (critical systems), sesuai dengan kebutuhan yang diutarakan oleh unit-unit kerja lainnya. Sistem utama ini akan merupakan layanan yang rnendapatkan prioritas lebih untuk pemulihannya saat keadaan darurat, dan disesuaikan dengan standar kualitas layanan yang diacukan.
j. Sistem utama untuk layanan yang diberikan oleh IT harus memiliki rencana pemulihan di tempat (*in site*) dalam bentuk *contingency plan*, dimana terdapat infrastruktur cadangan yang dapat digunakan untuk memberikan layanan serupa di saat layanan utama terganggu. Sistem utama dan cadangannya ini diperlukan dalam rangka IT untuk memenuhi standar kualitas layanan yang ditentukannya. Contoh dari pemulihan sistem secara ini misalnya dari hasil *backup data*, atau server lainnya dengan fungsi serupa yang dapat dikaryakan untuk sementara waktu.
k. Saat keadaan darurat ditetapkan oleh IMT, maka Unit Kerja IT akan membentuk suatu pusat komunikasi yang dapat digunakan oleh IMT dalam melakukan komunikasi dan koordinasinya untuk operasional Danareksa. Pusat komunikasi tersebut lebih diarahkan secara fungsi, dan tidak perlu berbentuk fasilitas fisik tersendiri. Pusat komunikasi ini juga mencakup komunikasi dengan pihak ketiga penyedia layanan.
l. Saat keadaan darurat ditetapkan oleh IMT, Unit Kerja IT harus secepatnya berusaha untuk memulihkan kembali kondisi kerja sistem utama sehingga layanan dan proses penting Unit-unit Kerja Danareksa dapat kembali dilakukan dari sistem utama di kantor pusat. Perkiraan waktu yang dibutuhkan adalah sekitar 5 (lima) hari, tergantung dari kondisi saat keadaan darurat ditetapkan.
m. Unit Kerja IT harus berusaha untuk memiliki suatu fasilitas tetap berupa DRC, yang dapat digunakan untuk memberikan layanan dan proses penting selama dalam keadaan darurat. Perkiraan waktu yang dibutuhkan untuk memindahkan layanan dari sistem utama ke sistem DRC adalah sekitar 4 (empat) sampai dengan 8 (delapan) jam.

n. Untuk mempercepat pemulihan layanan ini balk di DRC maupun di sistem utama di kantor pusat, dapat dibentuk suatu tim tersendiri dengan tugas khusus untuk mempercepat pencapaian tujuan di atas. Tim ini akan langsung bertanggung jawab kepada IMT, dengan tugas dan tanggung jawab sebagaimana didelegasikan oleh IMT. Tim ini bersifat *ad-hoc*, dan hanya bertugas sampai layanan dan proses penting kembali berjalan. Proses dan prosedur pembentukan serta operasionalisasi tim ini akan diatur secara terpisah.
o. Unit kerja IT juga harus mempersiapkan suatu kerangka tim yang akan menjalankan layanan dan proses penting IT selama keadaan darurat. Keanggotaan tim ini dapat diperluas secara bertahap sampai ke seluruh tim operasional IT dan Divisi terkait, sesuai dengan kapasitas dan kondisi yang dimungkinkan. Pada batas waktu yang ditetapkan untuk pemulihan layanan di atas, maka sebagian besar atau seluruh tim operasional IT dan Divisi terkait sudah berfungsi seperti sediakala.
p. Setelah keadaan darurat berakhir, maka Unit Kerja IT harus mendukung IMT dalam proses untuk transisi ke kondisi operasional normal. Jika layanan IT masih dilakukan dari DRC, maka harus dipersiapkan skenario pengembalian layanan tersebut ke sistem utama di kantor pusat. Hal ini akan dapat dilakukan jika sistem utama tersebut sudah kembali beroperasi normal.
q. Skenario transisi di atas harus sesuai dengan kerangka yang telah ditetapkan dalam dokumen BCP. Implementasi dari skenario ini harus dikoordinasikan oleh IMT dengan seluruh unit kerja lainnya yang menggunakan layanan IT untuk operasional mereka sehari-hari.
r. Setelah skenario transisi selesai dikerjakan, IMT dapat menyatakan bahwa kondisi operasional normal telah tercapai, dan keadaan darurat dinyatakan selesai.

XIII. MONITOR DAN EVALUASI PENGENDALIAN INTERNAL

XIII.1. IT *Assesment* dan *Penetration Test*

Tujuan

Memastikan seluruh jaringan server, *network*, perangkat keamanan jaringan, *operating system* dan aplikasi yang digunakan untuk menjalankan *core* aplikasi yang digunakan oleh perusahaan aman dari akses yang tidak terdaftar dan tidak bertanggung jawab.

Ruang Lingkup

Kebijakan ini mencakup seluruh jaringan *server*, *network*, *core* aplikasi dan aplikasi-aplikasi yang di publikasikan di Internet.

Kebijakan

a. Danareksa melakukan IT *Assessment* secara internal minimal 1 (satu) kali dalam 1 (satu) tahun.
b. Danareksa wajib melakukan IT *Assessment* dan *Penetration Test* minimal 1 (satu) kali dalam 1 (satu) tahun oleh *independent reviewer* yang mempunyai kompetensi dan pengalaman yang sesuai.
c. Pengadaan jasa *independent reviewer* tersebut di atas mengikuti kebijakan dan prosedur pengadaan oleh PT. Danareksa (Pesero).

XIII.2. IT *Compliance*

Tujuan

Memastikan seluruh kegiatan operasional atau layanan TI sesuai dengan kebijakan, prosedur, standar dan peraturan yang berlaku.

Ruang Lingkup

Kebijakan ini mencakup seluruh prosedur, instruksi kerja dan standar TI yang berlaku di Divisi IT Kantor Pusat dan SID-SID.

Kebijakan

a. Pihak IT memiliki unit yang berfungsi sebagai monitoring pelaksanaan kebijakan, prosedur, instruksi kerja dan standar layanan, infrastruktur dan operasi TI.
b. Pihak IT melakukan program *compliance* pengendalian internal atas pelaksanaan kebijakan, prosedur, instruksi kerja dan standar layanan, infrastruktur dan operasi TI minimal 1 (satu) kali pertahun.
c. Pihak IT membantu kegiatan evaluasi atau audit yang dikoordinasikan oleh Internal Audit Danareksa, *Independent Auditor Professional* maupun dari pihak lain yang kompeten.

XIV. MODEL *ASSESMENT*

Maturity model (COBIT 4) merupakan mekanisme *assesment* tata kelola TI untuk mengevaluasi tingkat penerapan tata kelola TI dalam suatu entitas atau perusahaan. Dalam *maturity model* tingkat penerapan tata kelola TI diukur dari pelaksanaan pengendalian internal yang dipetakan menurut 5 (lima) level pencapaian, dimana masing-masing menunjukkan kualitas pelaksanaan dari masing-masing pengendalian di dalam organisasi/unit kerja.

Peta pengelompokan masing-masing pengendalian internal disusun berdasarkan kontrol yang terdapat dalam Kebijakan yang berlaku, baik secara keseluruhan kontrol maupun dipilih menurut asesmen risiko yang telah disusun berdasarkan kondisi organisasi atau perusahaan.

Tingkatan dalam *maturity model* dapat disampaikan sebagai berikut:

Level *Maturity*	Keterangan
0	***Non-Eksis***, Proses tidak ada dan Organisasi tidak mengenali adanya Tata Kelola TI.
1	***Initial/AdHoc***, Proses kadang dilaksanakan/*Adhoc* (khusus) kasus demi kasus dan tidak ada standarisasi serta tidak terorganisir.
2	**Berulang**, Proses telah dibentuk namun belum ada koordinasi dari prosedur standar dan tanggung jawab serta tidak terdokumentasi.
3	**Terdefinisi**, Proses selalu dilaksanakan, standarisasi, terdokumentasi, dan dikomunikasikan.
4	**Terkelola**, Proses selalu dilaksanakan, terdokumentasi, dikomunikasikan, dikelola dengan baik serta dapat diukur pencapaiannya.
5	**Optimal**, Proses selalu dilaksanakan, terdokumentasi, dikomunikasikan,dikelola, dapat diukur dan dapat dioptimasi hasilnya sesuai dengan kebutuhan organisasi secara otomatis (dapat memanfaatkan *tool*).

Metoda pelaksanaan asesmen dilakukan melalui survei yang dilakukan terhadap para pelaku kontrol: pemilik proses, pengelola TI, maupun pengelola kebijakan TI pada suatu organisasi korporasi. Dalam beberapa kasus survei dilakukan terhadap karyawan yang dipilih sesuai dengan pertimbangan akuntabilitas pelaksanaan pengendalian internal sesuai dengan *job* posisi.

Pelaksana asesmen dapat dilakukan secara internal perusahaan (mandiri) atau secara independen dengan melibatkan pihak lain. Target *maturity level* dalam 5 (lima) tahun sesuai dengan rekomendasi kementerian BUMN dan mengacu kepada *best practice* standar di industri dunia adalah: Level 3 (tiga)

Catatan *maturity level* : Untuk mencapai target *maturity level* 3 dalam 5 tahun mungkin bisa tercapai dengan asumsi semua sumber daya/aspek yang dibutuhkan terpenuhi, antara lain dana, *people* (*skills and competency*, *quantity*), *tools*, *culture*, *management support*.
Sebaiknya poin dalam panduan kebijakan lebih ditekankan pada tujuan pentingnya maturity measurement, karena maturity measurement bukanlah tujuan akhir, lebih sebagai alat pendukung untuk pencapaian tujuan bisnis. Perlu diperhatikan bahwa dalam BUMN terdiri atas perusahan-perusahaan yang datang dalam industri yang beragam dan kondisi internal perusahaan yang berbeda (*capability*, *finance*, dan sebagainya). Untuk itu sebaiknya selain melihat pada *best practice*, juga melakukan *benchmark* pada industri yang sama, dan mendiskusikan terlebih dahulu untuk mencapai suatu kesepakatan bersama akan target *maturity level* yang hendak dituju pada tiap-tiap entitas.

Sebaiknya poin dalam Kebijakan lebih ditekankan pada tujuan pentingnya *maturity measurement*, karena *maturity measurement* bukanlah tujuan akhir, lebih sebagai alat pendukung untuk pencapaian tujuan bisnis. Perlu diperhatikan bahwa Danareksa terdiri atas perusahan-perusahaan yang datang dalam industri yang beragam dan kondisi internal perusahaan yang berbeda (*capability*, *finance*, dan sebagainya). Untuk itu sebaiknya selain melihat pada *best practice*, juga melakukan *benchmark* pada industri yang sama, dan mendiskusikan terlebih dahulu untuk mencapai suatu kesepakatan bersama akan target *maturity level* yang hendak dituju pada tiap-tiap BUMN.

XV. PANDUAN *CHECKLIST* TATA KELOLA IT

Panduan *checklist* tata kelola TI diberikan sebagai pedoman bagi perusahaan dalam melaksanakan implementasi tata kelola TI sebagai dasar pelaksanaan fungsi monitor dan evaluasi pengendalian internal (*internal control*) tata kelola TI. Pelaksanaan *checklist* diperlukan untuk memberikan jaminan mengenai operasi TI yang efektif dengan tingkat kepatuhan terhadap kebijakan dan aturan yang berlaku.

Komposisi pengisian *item* dalam *checklist* dapat berbeda untuk setiap entitas sesuai dengan kondisi dan tingkat *maturity* implementasi tata kelola TI di masing-masing entitas tersebut.

XV.1. *Checklist* sebagai fungsi monitor implementasi Kebijakan Strategis

No.	Kebijakan	Pelaksanaan		Bukti Dokumentasi		Komunikasi (Sosialisasi)	
1	Penetapan Peran TI Perusahaan	☐ ☐ ☐	Tidak ada Kadang ada Selalu ada	1 2	*Statement* (IT *Support*/IT *Enabler*) dalam dokumen strategi perusahaan (RJPP) *Key Performance Indicator* (KPI) dan/atau *Balance Score Card* (BSC)	☐ ☐	Ya Tidak
2	Perencanaan Perusahaan	☐ ☐ ☐	Tidak ada Kadang ada Selalu ada	1 2 3	IT *Strategic* BSC (1th, 3th s/d 5th) IT *Roadmap* IT *Master Plan*	☐ ☐	Ya Tidak
3	Kerangka Kerja Proses dan Organisasi TI	☐ ☐ ☐	Tidak ada Kadang ada Selalu ada	1 2 3	IT *Steering Committee* Pengelolaan IT *Policy* IT *Operation & Development* (*Procedure*)	☐ ☐	Ya Tidak

4	Pengelolaan Sumber Daya TI	☐ ☐ ☐	Tidak ada Kadang ada Selalu ada	1 2 3 4	Prosedur pengelolaan SDM: *a.* Kompetensi/*Job Description* b. Rumpun Jabatan/Struktur c. Pelatihan Prosedur Pengelolaan Data/Informasi Prosedur Pengelolaan *Hardware*/*Software* Prosedur Pengelolaan Infrastruktur (*Data Center*, *Network*, dsb).	☐ ☐	Ya Tidak
5	Pengelolaan Investasi TI	☐ ☐ ☐	Tidak ada Kadang ada Selalu ada	1 2 3 4	RKAP dan RJPP IT *Allignment* BSC *Horizontal Allignment* Prosedur Pengelolaan Pengadaan Investasi IT	☐ ☐	Ya Tidak
6	Pengelolaan Risiko TI	☐ ☐ ☐	Tidak ada Kadang ada Selalu ada	1 2 3	Prosedur *Risk Assessment* *Disaster Recovery Plan* *Disaster Recovery Center*	☐ ☐	Ya Tidak

XV.2. *Checklist* sebagai fungsi monitor implementasi Kebijakan Operasional

No.	Kebijakan	Pelaksanaan		Bukti Dokumentasi (*Evidence*)		Komunikasi (Sosialisasi)	
1	Pengelolaan Layanan TI	☐ ☐ ☐	Tidak ada Kadang ada Selalu ada	1 2 3	Prosedur Helpdesk Prosedur atau Standar Layanan TI (sistem manual) Implementasi ITIL (misalnya, *Service Desk*, *Incident Management*, *Change Management*)	☐ ☐	Ya Tidak

2	Pengelolaan Sekuriti IT	☐ Tidak ada ☐ Kadang ada ☐ Selalu ada		1 2	Standar atau *guideline* sekuriti yang umum digunakan dan *acceptable use of* IT *assets* seperti penggunaan e-mail, atau PC/Laptop Perusahaan Prosedur keamanan jaringan internal perusahaan dan hal lain yang perlu diatur pemakaiannya	☐ Ya ☐ Tidak	
3	Pengelolaan Layanan Pihak Ketiga	☐ Tidak ada ☐ Kadang ada ☐ Selalu ada		1 2 3	Pengelolaan perjanjian dan kontrak Tersedianya kontrak template untuk pengelolaan kontrak yang lebih profesional Laporan evaluasi dan monitoring perjanjian ke pihak ketiga	☐ Ya ☐ Tidak	
4	Monitor dan Evaluasi Kinerja TI	☐ Tidak ada ☐ Kadang ada ☐ Selalu ada		1 2	Prosedur pengukuran dan pelaporan kinerja TI Prosedur untuk monitor dan evaluasi kinerja (KPI)	☐ Ya ☐ Tidak	
5	Monitor dan Evaluasi Pengendalian Internal	☐ Tidak ada ☐ Kadang ada ☐ Selalu ada		1 2	Dokumen *Checklist* Tata Kelola TI Prosedur asesmen Tata Kelola TI dan evaluasi pihak ketiga	☐ Ya ☐ Tidak	
6	Pengelolaan *Compliance External Regulation* (*Optional*)	☐ Tidak ada ☐ Kadang ada ☐ Selalu ada		1 2	Standar Regulasi Eksternal (*Checklist*) Asesmen terhadap *External Compliance* yang dicapai	☐ Ya ☐ Tidak	

XVI. LAIN-LAIN

1. Yang dimaksud dengan KPR adalah sesuai dengan SK Direksi Nomor KD-40/004/DIR tentang Pembentukan Komite Pengelolaan Risiko PT Danareksa (Persero) tanggal 26 Januari 2016, beserta Surat Keputusan penggantinya.
2. Pelaksanaan Kebijakan yang tidak sesuai dengan ketentuan dalam Kebijakan ini harus mendapat persetujuan dari KPR.
3. Perusahaan Anak wajib mengacu pada Kebijakan Keamanan dan Keselamatan yang diatur dalam Keputusan ini untuk menetapkan Kebijakan Keamanan dan Keselamatannya.
4. Selama Perusahaan Anak belum menetapkan Kebijakan Keamanan dan Keselamatan, maka hal-hal terkait dengan keamanan dan keselamatan Perusahaan Anak wajib mengacu pada Keputusan ini.
5. Apabila dibutuhkan prosedur-prosedur yang mengatur secara detail aktivitas pekerjaan yang berkaitan dengan pelaksanaan Kebijakan ini, maka prosedur dan instruksi kerja kegiatan tersebut harus dibuat dengan mengacu kepada Kebijakan ini.
6. Apabila terjadi perubahan struktur transaksi dan regulasi yang menyebabkan batasan-batasan di dalam Surat Keputusan ini menjadi tidak memadai, maka akan dikeluarkan Surat Keputusan pengganti dengan persetujuan tertulis dari KPR.
7. Surat Keputusan ini berlaku sejak penandatanganan dokumen ini.