BERITA NEGARA REPUBLIK INDONESIA

No.256, 2010 LEMBAGA SANDI NEGARA. Pemanfaatan Teknologi Informasi.

PERATURAN KEPALA LEMBAGA SANDI NEGARA

REPUBLIK INDONESIA

NOMOR 13 TAHUN 2010

TENTANG

PEDOMAN PEMANFAATAN TEKNOLOGI INFORMASI

DI LEMBAGA SANDI NEGARA

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA LEMBAGA SANDI NEGARA REPUBLIK INDONESIA,

Menimbang : a. bahwa dalam rangka menunjang kelancaran pelaksanaan tugas pokok dan fungsi Lembaga Sandi Negara, diperlukan Teknologi Informasi yang memadai, baik dari segi SDM, perangkat keras maupun perangkat lunak, dengan mempertimbangkan aspek manfaat, keamanan serta aspek efisien dan efektif;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a perlu menetapkan Peraturan Kepala Lembaga Sandi Negara tentang Pedoman Pemanfaatan Teknologi Informasi di Lembaga Sandi Negara;

Mengingat : 1. Keputusan Presiden Nomor 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Lembaga Pemerintah Non

Departemen sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Presiden Nomor 64 Tahun 2005;

2. Peraturan Kepala Lembaga Sandi Negara Nomor OT.001/PERKA.122/2007 Tahun 2007 tentang Organisasi dan Tata Kerja Lembaga Sandi Negara;
3. Peraturan Kepala Lembaga Sandi Negara Nomor 7 Tahun 2009 tentang Visi dan Misi Lembaga Sandi Negara;
4. Peraturan Kepala Lembaga Sandi Negara Nomor 10 Tahun 2009 tentang Rencana Strategis Lembaga Sandi Negara Tahun 2010 – 2014;

MEMUTUSKAN:

Menetapkan : PERATURAN KEPALA LEMBAGA SANDI NEGARA TENTANG PEDOMAN PEMANFAATAN TEKNOLOGI INFORMASI DI LEMBAGA SANDI NEGARA.

Pasal 1

Pedoman Pemanfaatan Teknologi Informasi di Lembaga Sandi Negara sebagaimana tercantum dalam Lampiran Peraturan Kepala Lembaga Sandi Negara ini merupakan bagian yang tidak terpisahkan dari Peraturan Kepala Lembaga Sandi Negara ini.

Pasal 2

Pedoman Pemanfaatan Teknologi Informasi di Lembaga Sandi Negara sebagaimana dimaksud dalam Pasal 1 merupakan acuan bagi kegiatan yang berhubungan dengan pemanfaatan dan pengelolaan di bidang teknologi informasi di Lembaga Sandi Negara.

Pasal 3

Hal-hal yang belum diatur dalam Peraturan Kepala Lembaga Sandi Negara ini akan ditetapkan dalam peraturan tersendiri dan ditentukan kemudian.

Pasal 4

Peraturan Kepala Lembaga Sandi Negara ini mulai berlaku pada tanggal ditetapkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Kepala Lembaga Sandi Negara ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 10 Februari 2010

KEPALA LEMBAGA SANDI NEGARA
REPUBLIK INDONESIA,

WIRJONO BUDIHARSO

Diundangkan di Jakarta
pada tanggal 8 April 2010

MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

PATRIALIS AKBAR

DAFTAR ISI

PEDOMAN PEMANFAATAN TEKNOLOGI INFORMASI
DI LEMBAGA SANDI NEGARA

BAB I
PENDAHULUAN

A. Umum

Kemajuan teknologi yang demikian pesat, khususnya Teknologi Informasi (TI) telah memberikan kontribusi besar di beberapa bidang, dan membuat informasi dapat diperoleh dengan cepat dan mudah. Implementasi TI dapat digunakan untuk mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengirimkan, mengumumkan dan/atau menyebarkan informasi.

Lembaga Sandi Negara (Lemsaneg) memanfaatkan TI dalam rangka melaksanakan tugas pemerintahan di bidang persandian. Dalam perkembangannya, Lemsaneg telah mengembangkan berbagai macam aplikasi Sistem Informasi (SI) berbasis TI, agar informasi yang disajikan akan semakin handal, akurat dan tepat waktu.

Agar pelaksanaan pemanfaatan TI di Lemsaneg tidak menimbulkan permasalahan maka perlu diatur tentang pemanfaatan dan pengelolaan TI yang dapat dijadikan pedoman dalam pelaksanaan tugas di lingkungan Lemsaneg.

B. Maksud dan Tujuan

Pedoman ini dibuat dengan maksud sebagai acuan dalam mengelola dan memanfaatkan TI di lingkungan Lemsaneg dengan tujuan agar pengelolaan dan pemanfaatan TI di lingkungan Lemsaneg dapat terwujud secara efektif dan efisien.

C. Pengertian

Dalam pedoman ini yang dimaksud dengan :

1. *Access Control* adalah mekanisme pengontrolan atau pembatasan akses terhadap *resource* seperti server, direktori, dan *file* dengan melakukan proses otorisasi terhadap *user* yang mengakses *resource* tersebut.
2. *Access Point* yang selanjutnya disebut AP adalah tempat (*point*) yang menjadi pusat dari beberapa koneksi terhubung.
3. *Antivirus* adalah program untuk melacak keberadaan dan mengamankan virus pada media penyimpanan, baik pada disk maupun memori aplikasi.
4. *Antispam* adalah program untuk mengamankan dari pesan yang tidak diinginkan atau pesan sampah

5. *Asset* adalah entitas yang bernilai pada dunia usaha atau *enterprise*, dapat berupa prosesor komputer, disk, link jaringan, program, datum atau *user*.
6. *Asynchronous Transfer Mode (ATM) Switch* adalah teknologi yang diterapkan pada jaringan untuk melakukan proses transmisi data, suara dan lain-lain secara *real time*.
7. *Authenticity* adalah keautentikan atau keaslian.
8. *Availability* adalah ketersediaan dan keterjaminan sumber daya sistem komputer bagi pihak-pihak yang mendapat otoritas saat diperlukan.
9. *Backup System* adalah sistem dan prosedur yang dibuat untuk mengatasi segala permasalahan (bencana) yang mungkin timbul mencakup penyiapan *backup* baik perangkat keras ataupun lunak dari sistem yang dioperasikan.
10. *Bridge* adalah perangkat yang menghubungkan jaringan secara fisik dengan cara menggabungkan dua buah LAN yang menggunakan protokol sejenis dan mampu mengawasi lalu lintas data sehingga dapat memberikan informasi tentang volume lalu lintas dan kesalahan jaringan.
11. *Browsing tools* adalah alat untuk penjelajahan situs di Internet.
12. *Chatting* adalah percakapan interaktif melalui teks maupun suara antar sesama pengguna komputer yang terhubung dalam suatu jaringan.
13. *Client* adalah komputer yang memanfaatkan *resource* dalam jaringan yang disediakan oleh server.
14. *Computer security* adalah keamanan sistem komputer yang terbagi menjadi keamanan eksternal, keamanan *interface* pemakai dan keamanan internal.
15. *Confidentiality* adalah kerahasiaan.
16. *Database* adalah kumpulan informasi yang disimpan di dalam komputer secara sistematik sehingga dapat diperiksa menggunakan suatu program komputer untuk memperoleh informasi dari *database* tersebut.
17. *Database server* adalah sebuah *node* atau titik pada sebuah jaringan komputer yang dikhususkan untuk menyimpan *database* bersama dan memproses permintaan *database* yang dikirimkan oleh pengguna pada *node* lain.
18. *Data center* disebut dengan Pusat Komputerisasi adalah pusat pemrosesan data yang didukung dengan perangkat pengolahan data tersebut.
19. *Denial of Service* yang selanjutnya disebut DoS adalah serangan virus atau *hacker* yang masuk ke dalam sistem komputer tanpa melalui akses resmi sesuai prosedur dan mengacaukan fungsi kerja normal sebuah sistem.
20. *Dial-up* adalah jenis komunikasi yang menggunakan modem dan saluran telepon biasa untuk bisa berhubungan antara komputer yang satu dengan komputer yang lain, atau

bisa juga berarti *provider* Internet yang memanfaatkan saluran telepon sebagai saluran utamanya.

21. *Digital Certificate* adalah sertifikat yang dikeluarkan oleh pihak yang dipercaya, yang berfungsi untuk mengenali identitas sebuah perusahaan atau individu dalam suatu jaringan yang mengandung informasi nama identitas, kunci dasar (untuk enkripsi), dan pengesahan bentuk lain.
22. *Disaster Recovery Plan* yang selanjutnya disebut DRP adalah rencana penanggulangan atau pemulihan musibah atau bencana, seperti kebakaran, gempa bumi dan lain sebagainya yang terjadi terhadap suatu sistem.
23. *Electronic Commerce* adalah kumpulan teknologi, aplikasi, dan *business process* yang menghubungkan perusahaan, konsumen, dan komunitas melalui transaksi elektronis dan pertukaran barang, servis dan informasi secara elektronis.
24. *Electronic Mail* (e-mail) sistem adalah surat elektronik melalui jaringan Lemsaneg (intranet) dan/atau melalui jaringan publik (internet untuk keperluan tukar menukar pesan atau informasi) di lingkungan Lemsaneg.
25. *Ethernet* adalah suatu standar perangkat keras LAN, mengenai pengkabelan serta spesifikasi transmisinya.
26. *Firewall* adalah sebuah *software* yang dipasang pada sebuah jaringan dan berfungsi memproteksi sistem komputer dengan tujuan mengamankan jaringan internal.
27. *Frame Relay* adalah protokol WAN yang dapat menghubungkan beberapa perangkat jaringan dengan *multipoint* WAN.
28. *Hub* adalah perangkat jaringan komputer yang berfungsi untuk menghubungkan peralatan-peralatan dengan *ethernet* atau serat optik sehingga menjadikannya dalam satu segmen jaringan.
29. Infrastruktur adalah sarana dan prasarana yang terdiri dari perangkat keras, perangkat lunak seperti OS, aplikasi *middleware* dan *database*.
30. *Integrity* adalah integritas.
31. *Isolation* adalah penghambatan atau pemisahan suatu hal dari hal lain.
32. *Layer* adalah lapisan (konsep) dalam *networking*.
33. *Local Area Network* yang selanjutnya disebut LAN adalah sistem komunikasi data setempat atau lokal dalam bentuk jaringan komputer dalam suatu ruangan, gedung atau lokasi tertentu yang dihubungkan dengan saluran komunikasi secara khusus.
34. *Logic Bomb* adalah program perusak yang ditempelkan pada program komputer resmi untuk memeriksa suatu kumpulan kondisi di sistem ketika kondisi-kondisi yang dimaksud ditemui, maka akan mengeksekusi suatu fungsi yang menghasilkan aksi-aksi

tak diotorisasi seperti mengubah atau menghapus data atau seluruh *file*, menyebabkan mesin berhenti, atau mengerjakan perusakan lain.

35. *Login* adalah proses untuk masuk ke dalam sebuah layanan *online* yang berisi nama dan *password.*
36. *Mac Address* adalah pengalamatan perangkat keras dari sebuah *device* dalam jaringan skala medium, dan telah distandarkan.
37. *Mailbox* adalah *s*uatu lokasi memori yang menyimpan data yang berhubungan dengan surat menyurat elektronik.
38. *Mail server* adalah perangkat lunak program yang mendistribusikan *file* atau informasi sebagai respons atas permintaan yang dikirim via surat elektronik, juga digunakan pada *bitnet* untuk menyediakan layanan serupa FTP.
39. *Malware* adalah perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer atau jejaring komputer yang berniat jahat dan tidak diinginkan.
40. *Metropolitan Area Network* yang selanjutnya disebut MAN adalah jaringan komputer dan beberapa komputer atau LAN yang saling berhubungan satu sama lain, dimana jaringan komputer tersebut berada di berbagai tempat atau gedung namun masih dalam satu kota yang sama.
41. *Multiplexer* adalah alat atau komponen elektronika yang bisa memilih input (masukan) yang akan diteruskan ke bagian output (keluaran). Pemilihan *input* mana yang dipilih akan ditentukan oleh signal yang ada di bagian kontrol.
42. *Network Interface Card* yang selanjutnya disebut NIC adalah perangkat keras yang dipasang pada komputer agar komputer tersebut bisa terhubung ke komputer lain.
43. *Network Monitoring* adalah kegiatan memonitor jaringan komputer jika lambat atau terdapat komponen yang gagal berfungsi.
44. Otorisasi adalah proses untuk pengecekan apakah seseorang berhak atas penggunaan suatu sistem.
45. Paket data adalah dalam network TCP/IP (internet), data yang dikirim ke komputer lain dipecah-pecah menjadi paket-paket yang kecil.
46. Penanggung Jawab adalah pimpinan unit atau bagian yang bertanggung jawab terhadap layanan TI di Lemsaneg, dalam hal ini Kepala Bagian Hubungan Masyarakat dan Kerjasama.
47. Pengelola adalah suatu unit atau bagian dibawah unit atau bagian Penanggung Jawab, dan mempunyai tugas pokok sebagai Pengelola layanan TI Lemsaneg.
48. Pengguna adalah semua pegawai, dan/atau pihak lain yang atas persetujuan Pengelola menggunakan layanan TI di lingkungan Lemsaneg.

49. Perangkat Lunak Aplikasi adalah suatu program komputer yang dibuat untuk melaksanakan tugas-tugas tertentu.
50. *Peripheral* adalah perangkat *input* atau *output* yang merupakan bagian dan pendukung sistem seperti printer, modem, *scanner* atau termasuk juga kamera digital.
51. *Private Branch Exchange* yang selanjutnya disebut PBX adalah sebuah sistem *switching* telepon internal yang digunakan untuk menghubungkan satu *extension* dengan *extension* lainnya maupun dengan jaring telepon publik.
52. *Private Key* adalah istilah yang sering digunakan untuk merujuk baik kunci yang diketahui bersama dalam sistem enkripsi simetrik atau bagian yang dirahasiakan dari pasangan kunci yang digunakan pada sistem asimetrik.
53. *Proxy* adalah mekanisme dimana satu sistem menyediakan diri untuk sistem lain sebagai tanggapan atas permintaan untuk suatu protokol.
54. *Repudiation* adalah penyangkalan oleh entitas sistem yang dilibatkan dalam asosiasi khusus asosiasi yang mentransfer informasi.
55. *Repeater* adalah alat yang berfungsi untuk memperpanjang rentang jaringan dengan cara memperkuat isyarat elektronis.
56. *Router* adalah perangkat yang berfungsi menghubungkan dua atau lebih *network* yang berbeda.
57. *Security System* adalah sistem yang digunakan untuk pengamanan fisik dan pengamanan logik terhadap teknologi informasi.
58. *Segmentation* adalah pemecahan jaringan komputer ke dalam *subnetwork*.
59. Server adalah komputer yang bertugas sebagai pelayan jaringan yang mengatur lalu lintas data dalam sebuah jaringan dan menyediakan *resource* yang dapat dipakai oleh komputer lain yang terhubung dalam jaringannya.
60. Sistem Operasi yang selanjutnya disebut OS adalah perangkat lunak sistem yang mengatur dan mengendalikan perangkat keras dan memberikan kemudahan penggunaan komputer ke pemakai.
61. Sistem Utama adalah sistem yang mencatat kegiatan operasional Lemsaneg dan aset-aset utama Lemsaneg seperti sistem informasi hasil pengawasan, sistem informasi kepegawaian, sistem informasi keuangan dan perlengkapan dan sistem-sistem lainnya yang telah setujui oleh Kepala Lemsaneg atau pejabat yang mendapat prioritas pemulihan pada kondisi darurat.
62. Sistem *log* adalah catatan-catatan yang berkaitan dengan akses ke suatu sistem.
63. Situs adalah sebuah komputer yang terhubung oleh internet, dan menyajikan informasi atau layanan, seperti *newsgroups*, *e-mail*, atau halaman web.

64. *Script* adalah program yang ditulis dalam bahasa pemrograman khusus dan biasanya terdiri dari serangkaian perintah.
65. *Sniffing* adalah suatu tindakan para penyusup untuk mengetahui isi data melalui internet dengan memasukkan program *Packet Sniffer* untuk mendapatkan *account name* dan *password* yang bisa digunakan.
66. *Software Security* adalah utiliti atau pengembangan perangkat lunak dan program atau aplikasi yang memproteksi data yang dimiliki sistem.
67. *Spam* adalah pesan yang tidak diinginkan atau pesan sampah.
68. *Spoofing* adalah suatu tindakan penyusupan dengan menggunakan identitas resmi secara ilegal sehingga dapat mengakses segala sesuatu dalam jaringan.
69. *Switch* adalah perangkat jaringan yang bekerja dilapisan *Data-link*, mirip dengan *bridge*, berfungsi menghubungkan banyak segmen LAN ke dalam satu jaringan yang lebih besar.
70. Tim Audit TI adalah tim profesional yang tugasnya untuk menyatakan validitas, reliabilitas dan integritas dari semua aspek lingkungan sistem atau teknologi informasi komputer sebuah organisasi.
71. *Trojan Horse* adalah sebuah aplikasi yang didesain untuk melakukan sebuah kecurangan namun terselubung seperti menyelipkan (*attach file* lewat *e-mail*) sebuah *file* tertentu yang mengandung *Trojan Horse* setelah berhasil menginfeksi maka bisa dipastikan *hacker* bisa mendapat akses tak terhingga ke komputer korban.
72. *User ID* adalah simbol atau karakter string yang unik, digunakan oleh sistem untuk mengidentifikasi *user* tertentu.
73. Validasi Data adalah menguji dan mencetak kebenaran dari suatu data transaksi.
74. *Virtual Private Network* yang selanjutnya disebut VPN adalah jaringan komputer secara logik yang dibangun dari sumber daya sistem yang relatif umum, jaringan fisik (seperti internet) seringkali menggunakan enkripsi.
75. *Voice over Internet Protocol* yang selanjutnya disebut VoIP adalah teknologi yang memungkinkan percakapan suara jarak jauh melalui media internet.
76. *Web Browsing* adalah suatu program komputer yang menyediakan fasilitas untuk menjelajah situs di internet.
77. *Web site* adalah suatu koleksi dokumen HTML pribadi atau perusahaan dalam server web.
78. *Wide Area Network* yang selanjutnya disebut WAN merupakan suatu jaringan digunakan untuk menghubungkan komunikasi data dan suara antara dua LAN atau lebih.

79. *Wireless LAN* yang selanjutnya disebut WLAN adalah suatu jaringan area lokal nirkabel (tanpa kabel) yang menggunakan gelombang radio sebagai media transmisinya untuk memberi sebuah koneksi jaringan ke seluruh pengguna dalam area sekitar.
80. *Worm* adalah suatu program yang dapat mereplikasi dirinya dengan menggunakan media komputer yang bersifat dekstruktif terhadap *disk* dan memori serta menyebabkan kerusakan pada sistem dan memperlambat kinerja komputer dalam mengaplikasi sebuah program.

D. Ruang Lingkup

Pedoman Pemanfaatan TI menjelaskan tentang pemanfaatan dan pengelolaan aset dan layanan TI yang dimiliki Lemsaneg. Pedoman pemanfaatan TI diberlakukan bagi Pengguna, Pengelola dan Penanggung Jawab TI di Lemsaneg.

BAB II

LAYANAN TEKNOLOGI INFORMASI

DI LEMBAGA SANDI NEGARA

A. LAN

1. Aset LAN

Aset LAN terdiri dari *modem, Router*, *Switch*, *Hub, Bridge, Repeater, NIC* dan *AP.*

2. Pemanfaatan LAN

a. Pengguna LAN diperbolehkan :
   1) Memanfaatkan LAN guna mendukung tugas dan pekerjaan untuk kepentingan dinas;
   2) Mengajukan persetujuan tertulis kepada Penanggung Jawab dan melakukan koordinasi dengan Pengelola dalam hal:
      a) Implementasi perangkat atau aplikasi di lingkungan Lemsaneg yang membutuhkan LAN;
      b) Pemanfaatan LAN untuk kepentingan dinas yang bersifat khusus;
      c) Pemanfaatan LAN oleh mitra kerja dan tamu di Lemsaneg;
      d) Pemanfaatan LAN Lemsaneg menggunakan komputer pribadi;
      e) Melakukan *remote access* melalui fasilitas VPN terhadap LAN Lemsaneg guna kepentingan dinas;
      f) Menambahkan aset pada LAN Lemsaneg;
      g) Memindahkan segala infrastruktur LAN Lemsaneg.

b. Pengguna LAN dilarang untuk :
   1) Melakukan tindakan yang menyebabkan terganggunya aspek *Authenticity*, *Integrity*, *Availability* dan *Confidentiality* atas layanan LAN Lemsaneg;
   2) Melakukan tindakan yang mengganggu kepentingan umum dan kenyamanan pengguna lain;
   3) Melakukan perubahan baik sebagian maupun seluruh konfigurasi infrastruktur LAN Lemsaneg;
   4) Melakukan *DOS, Sniffing, Spoofing* dan meletakkan *Malware* seperti *virus, Worm, Trojan Horse* dan *Logic Bomb* pada LAN Lemsaneg;
   5) Melakukan pencurian terhadap sebagian atau seluruh aset LAN Lemsaneg.

3. Pengelolaan LAN

a. Tugas dan Wewenang Penanggung Jawab

1) Tugas Penanggung Jawab

Menjamin aspek *Authenticity, Integrity, Availability dan Confidentiality* serta menjamin keamanan seluruh aset LAN Lemsaneg.

2) Wewenang Penanggung Jawab

Memberikan sanksi kepada Pengelola dan Pengguna LAN jika terjadi pelanggaran dan/atau kelalaian yang menyebabkan terjadinya gangguan terhadap aspek *Authenticity, Integrity, Availability dan Confidentiality* pada LAN Lemsaneg.

b. Tugas dan Wewenang Pengelola

1) Tugas Pengelola

a) Mengelola seluruh aset LAN Lemsaneg dan melaksanakan koordinasi dengan unit kerja lain terkait pengamanan fisik dalam rangka pengamanan aset LAN Lemsaneg;

b) Melakukan pemantauan terhadap LAN Lemsaneg dan melaporkan segala kejadian khusus atau kejanggalan atas hasil pemantauan yang terjadi kepada Penanggung Jawab;

c) Membuat dokumentasi kegiatan, perubahan konfigurasi dan hasil pemantauan LAN Lemsaneg secara berkala;

d) Melaporkan kepada Penanggung Jawab, baik tertulis maupun tidak tertulis, jika terjadi gangguan terhadap aspek *Authenticity, Integrity, Availability dan Confidentiality* pada layanan LAN Lemsaneg;

e) Melaksanakan pengamanan infrastruktur LAN Lemsaneg dengan:

(1) Melakukan *compartmentalization, isolation, segmentation*;

(2) Menggunakan perangkat pengamanan jaringan;

(3) Menggunakan perangkat monitoring jaringan.

2) Wewenang Pengelola

a) Merubah konfigurasi infrastruktur LAN Lemsaneg, setelah mendapat persetujuan dari Penanggung Jawab dengan menyertakan alasan secara tertulis;

b) Melakukan *remote acces* dari dalam terhadap infrastruktur LAN Lemsaneg dalam rangka pemantauan dan konfigurasi;

c) Melakukan *remote access* dari luar melalui fasilitas VPN terhadap infrastruktur LAN Lemsaneg dalam rangka pemantauan dan konfigurasi;

d) Memberikan sanksi kepada Pengguna LAN setelah mendapat persetujuan Penanggung Jawab LAN;

e) Melakukan pemantauan lalu-lintas Paket Data yang melalui LAN Lemsaneg, dan melakukan pemeriksaan terhadap isi dari Paket Data jika ditemukan kejanggalan terhadap Paket Data tersebut.

3) Pengelola dilarang menyewakan, menjual dan melakukan tindakan lain terhadap sebagian atau seluruh infrastruktur LAN Lemsaneg untuk kepentingan komersial.

B. WAN

1. Aset WAN

Aset WAN terdiri dari *Router*, *ATM Switch*, *switch X.25/Frame Relay*, *modem, Multiplexer* dan *communication server.*

2. Pemanfaatan WAN

a. Pengguna WAN diperbolehkan:

1) Memanfaatkan WAN Lemsaneg guna mendukung tugas dan pekerjaan untuk kepentingan dinas;

2) Mengajukan ijin tertulis kepada Penanggung Jawab dan melakukan koordinasi dengan Pengelola dalam hal:

a) Pemanfaatan WAN untuk menghubungkan komunikasi data dan suara antara 2 (dua) LAN atau lebih;

b) Melakukan *remote access* melalui fasilitas VPN terhadap WAN Lemsaneg untuk keperluan dinas;

c) Implementasi perangkat atau aplikasi di lingkungan Lemsaneg yang membutuhkan WAN;

d) Pemanfaatan WAN untuk kepentingan uji coba, pendidikan dan pelatihan yang bersifat khusus;

e) Pemanfaatan WAN oleh mitra kerja dan tamu di Lemsaneg;

f) Melakukan penambahan perangkat jaringan pada WAN Lemsaneg.

b. Larangan bagi Pengguna WAN:

1) Melakukan tindakan yang dapat menyebabkan terganggunya aspek *Authenticity, Integrity, Availability dan Confidentiality* WAN Lemsaneg;

2) Melakukan tindakan yang mengganggu kepentingan umum dan kenyamanan Pengguna lain;

3) Melakukan perubahan baik sebagian maupun seluruh konfigurasi infrastruktur WAN Lemsaneg;

4) Melakukan *DOS, Sniffing, Spoofing* dan meletakkan *Malware seperti virus, Worm, Trojan Horse* da*n Logic Bomb* pada WAN Lemsaneg;

5) Melakukan pencurian terhadap sebagian atau seluruh aset WAN Lemsaneg.

3. Pengelolaan WAN

a. Tugas dan Wewenang Penanggung Jawab WAN

1) Tugas Penanggung Jawab

Menjamin aspek *Authenticity, Integrity, Availability dan Confidentiality* serta menjamin keamanan seluruh aset WAN Lemsaneg.

2) Wewenang Penanggung Jawab WAN

Memberikan sanksi kepada Pengelola dan Pengguna WAN jika terjadi pelanggaran dan/atau kelalaian yang menyebabkan terjadinya gangguan terhadap aspek *Authenticity, Integrity, Availability dan Confidentiality* pada WAN Lemsaneg.

b. Tugas dan wewenang Pengelola WAN

1) Tugas Pengelola WAN

a) Mengelola seluruh aset WAN Lemsaneg dan melaksanakan koordinasi dengan unit kerja terkait pengamanan fisik dalam rangka mengamankan seluruh aset WAN Lemsaneg;

b) Melaporkan kepada Penanggung Jawab, baik secara tertulis maupun tidak tertulis, jika terjadi gangguan terhadap aspek A*uthenticity, Integrity*, A*vailability* dan *Confidentiality* pada layanan WAN Lemsaneg;

c) Melakukan pemantauan terhadap WAN Lemsaneg dan melaporkan segala kejadian khusus atau kejanggalan atas hasil pemantauan yang terjadi kepada Penanggung Jawab;

d) Membuat dokumentasi seluruh kegiatan perubahan konfigurasi dan hasil pemantauan WAN Lemsaneg secara berkala.

2) Wewenang Pengelola WAN :

a) Merubah konfigurasi infrastruktur WAN Lemsaneg, setelah mendapat persetujuan Penanggung Jawab WAN Lemsaneg dengan menyertakan alasan secara tertulis;

b) Melakukan *remote access* dari dalam terhadap infrastruktur WAN Lemsaneg dalam rangka pemantauan dan konfigurasi;

c) Melakukan *remote access* dari luar melalui fasilitas VPN terhadap infrastruktur WAN Lemsaneg dalam rangka pemantauan dan konfigurasi;

d) Melakukan pemantauan lalu-lintas Paket Data yang melalui WAN Lemsaneg, dan melakukan pemeriksaan terhadap seluruh Paket Data jika ditemukan kejanggalan terhadap Paket Data tersebut;

e) Memberikan sanksi kepada Pengguna WAN jika ditemukan pelanggaran yang dilakukan Pengguna WAN setelah mendapat persetujuan Penanggung Jawab WAN.

3) Pengelola dilarang menyewakan, menjual dan melakukan tindakan lain terhadap sebagian atau seluruh infrastruktur WAN Lemsaneg untuk kepentingan komersial.

C. Layanan Internet

1. Koneksi Internet

a. Aset Koneksi Internet

Aset koneksi internet terdiri dari *Router, modem, bandwidth manager*, dan kapasitas akses internet yang disediakan *Internet Service Provider* (ISP).

b. Pemanfaatan Koneksi Internet

1) Pengguna layanan internet diperbolehkan:
   a) Memanfaatkan layanan internet Lemsaneg guna mendukung tugas dan pekerjaan untuk kepentingan dinas;
   b) Melakukan hal-hal sebagai berikut setelah mendapatkan persetujuan tertulis dari Penanggung Jawab:
      (1) Implementasi atau instalasi perangkat atau aplikasi di lingkungan Lemsaneg yang membutuhkan koneksi internet;
      (2) Pemanfaatan layanan internet untuk kepentingan uji coba, pendidikan dan pelatihan yang bersifat khusus;
      (3) Pemanfaatan layanan internet oleh mitra kerja dan tamu di Lemsaneg.
2) Pengguna layanan internet dilarang untuk:
   a) Melakukan tindakan yang dapat menyebabkan terganggunya aspek *Availability* layanan internet Lemsaneg;
   b) Melakukan tindakan yang mengganggu kepentingan umum dan kenyamanan pengguna lain;
   c) Melakukan *DOS, Sniffing, Spoofing* dan meletakkan *Malware seperti virus, Worm, Trojan Horse* dan *Logic Bomb* pada layanan internet Lemsaneg.

c. Pengelolaan Koneksi Internet

1) Tugas dan Wewenang Penanggung Jawab Koneksi Internet
   a) Tugas Penanggung Jawab
      Menjamin aspek *Availability* serta menjamin keamanan seluruh aset layanan internet Lemsaneg.
   b) Wewenang Penanggung Jawab Koneksi Internet

Menjatuhkan sanksi kepada Pengguna dan Pengelola internet jika terjadi gangguan terhadap aspek *Availability* pada layanan internet Lemsaneg.

2) Tugas dan Wewenang Pengelola Koneksi Internet
   a) Tugas Pengelola Koneksi Internet
      (1) Melakukan koordinasi dengan unit kerja lain dalam rangka mengamankan seluruh aset internet Lemsaneg;
      (2) Melaporkan kepada Penanggung Jawab, baik secara tertulis maupun tidak tertulis, jika terjadi gangguan terhadap aspek *Availability* layanan internet Lemsaneg;
      (3) Melakukan pemantauan terhadap lalu lintas penggunaan internet Lemsaneg;
      (4) Membuat dokumentasi seluruh kegiatan hasil pemantauan internet Lemsaneg secara berkala;
      (5) Melaporkan segala kejadian khusus hasil pemantauan yang terjadi pada internet Lemsaneg kepada Penanggung Jawab.
   b) Wewenang Pengelola Koneksi Internet
      (1) Memantau seluruh Paket Data yang melalui koneksi internet dan berhak melakukan pemeriksaan terhadap isi Paket Data tersebut jika ditemukan kejanggalan terhadap Paket Data tersebut;
      (2) Memberikan sanksi kepada Pengguna internet jika ditemukan pelanggaran yang dilakukan Pengguna internet setelah mendapat persetujuan Penanggung Jawab;
      (3) Melakukan koordinasi dengan pihak ISP pada keadaan tertentu, setelah mendapat persetujuan Penanggung Jawab.
   c) Pengelola dilarang menyewakan, menjual dan melakukan tindakan lain terhadap layanan internet Lemsaneg untuk kepentingan komersial.

2. Surat Elektronik

a. Aset surat elektronik

Aset surat elektronik Lemsaneg terdiri dari *Mail Server*, *web mail server*, isi surat elektronik, *Antispam*, aplikasi *Mail Server* dan *web mail.*

b. Pemanfaatan surat elektronik

1) Penamaan akun surat elektronik Lemsaneg menggunakan format (namajabatan)@lemsaneg.go.id dan/atau (namauser)@lemsaneg.go.id.
2) Penggunaan surat elektronik hanya untuk mendukung tugas dan pekerjaan yang berkaitan dengan kepentingan dinas.

3) Pengguna surat elektronik Lemsaneg diperbolehkan:
   a) Memiliki surat elektronik dengan kapasitas *Mailbox* sebagaimana ditetapkan oleh Penanggung Jawab;
   b) Mengajukan ijin tertulis kepada Penanggung Jawab dan melakukan koordinasi dengan Pengelola dalam hal:
      (1) Implementasi perangkat atau aplikasi di lingkungan Lemsaneg yang membutuhkan surat elektronik;
      (2) Pemanfaatan surat elektronik untuk kepentingan uji coba, pendidikan dan pelatihan yang bersifat khusus;
      (3) Menggunakan fasilitas VPN yang disediakan oleh Lemsaneg jika melakukan akses surat elektronik dari luar kantor Lemsaneg.
4) Kewajiban Pengguna surat elektronik Lemsaneg
   a) Mengelola *Mailbox* masing-masing, termasuk menghapus pesan-pesan yang sudah tidak diperlukan;
   b) Mempertanggungjawabkan isi atau pesan surat elektronik yang dibuatnya termasuk jika terjadi tuntutan hukum atas isi pesan tersebut;
   c) Bersikap waspada terhadap *attachment* dalam surat elektronik yang diterima dari alamat yang tidak dikenal atau tidak berkaitan dengan dinas dan melaporkan atau menyampaikan surat elektronik tersebut kepada Pengelola untuk diperiksa.
5) Pengguna surat elektronik Lemsaneg dilarang:
   a) Membuat dan penyebaran surat berantai (*chain letters);*
   b) Membahas hal-hal yang berkaitan dengan kegiatan politik;
   c) Menyampaikan pesan yang isinya bertentangan dengan hukum, aturan, dan kode etik, termasuk pelecehan dan ancaman;
   d) Menyampaikan pesan yang berasal dari sumber yang tidak dapat dipertanggung jawabkan kebenarannya, seperti surat kaleng, rumor, dan sejenisnya;
   e) Mengirim pesan yang tidak berkaitan dengan kegiatan dinas.

c. Pengelolaan surat elektronik

1) Penanggung Jawab dan Pengelola tidak dapat dituntut secara hukum berkenaan dengan isi pesan yang dibuat oleh Pengguna surat elektronik Lemsaneg.
2) Tugas dan Wewenang Penanggung Jawab surat elektronik
   a) Tugas Penanggung Jawab surat elektronik

Menjamin aspek A*uthenticity, Integrity*, *Availability,* dan *Confidentiality* serta menjamin keamanan seluruh aset layanan surat elektronik Lemsaneg.

b) Wewenang Penanggung Jawab surat elektronik
Memberikan sanksi kepada Pengguna dan Pengelola surat elektronik jika terjadi gangguan terhadap aspek *Authenticity, Integrity*, *Availability,* dan *Confidentiality* pada layanan surat elektronik Lemsaneg.

3) Tugas dan Wewenang Pengelola surat elektronik
a) Tugas Pengelola surat elektronik
(1) Melakukan koordinasi dengan unit kerja lain dalam rangka mengamankan seluruh aset surat elektronik Lemsaneg;
(2) Melaporkan kepada Penanggung Jawab, baik secara tertulis maupun tidak tertulis, jika terjadi gangguan terhadap aspek *Authenticity, Integrity*, *Availability,* dan *Confidentiality* pada layanan surat elektronik Lemsaneg;
(3) Melakukan pemantauan lalu lintas dan penggunaan surat elektronik Lemsaneg;
(4) Membuat dokumentasi seluruh kegiatan perubahan konfigurasi dan hasil pemantauan surat elektronik Lemsaneg secara berkala;
(5) Melaporkan segala kejadian khusus atau kejanggalan hasil pemantauan yang terjadi pada layanan surat elektronik Lemsaneg kepada Penanggung Jawab;
(6) Mengelola *Mailbox* pengguna surat elektronik dengan berupaya mencatat dan menyimpan dalam server *(e-mail server)* dan/atau media penyimpanan *backup* atas pesan surat elektronik yang telah dihapus oleh pengguna.

b) Wewenang Pengelola surat elektronik
(1) Merubah konfigurasi sistem surat elektronik Lemsaneg, setelah mendapat ijin dari Penanggung Jawab dengan menyertakan alasan secara tertulis;
(2) Melakukan *remote access* melalui fasilitas VPN terhadap layanan surat elektronik Lemsaneg dalam rangka pemantauan dan konfigurasi;
(3) Melakukan pemantauan terhadap seluruh surat elektronik yang melalui infrastruktur komputer Lemsaneg serta melakukan pemeriksaan jika ditemukan kejanggalan terhadap surat elektronik dimaksud;
(4) Melakukan perubahan atas pembatasan ukuran *Mailbox*, waktu pemakaian, dan hal-hal lain demi kepentingan Lemsaneg dengan memperhatikan ketersediaan sumber daya sistem yang ada setelah mendapat persetujuan Penanggung Jawab;

(5) Memberikan sanksi kepada Pengguna jika ditemukan pelanggaran yang dilakukan oleh Pengguna surat elektronik setelah mendapat persetujuan dari Penanggung Jawab;

(6) *Back up* data surat elektronik hanya dapat *di-restore* dan digunakan untuk keperluan pemulihan pada kondisi *disaster* dan/atau untuk kepentingan Lemsaneg.

c) Pengelola surat elektronik tidak diperbolehkan menyewakan, menjual dan hal lain yang bersifat komersial terhadap sebagian atau seluruh aset surat elektronik Lemsaneg.

3. Pemanfaatan Web Browsing

Ketentuan dan larangan

a. *Web Browsing* dimanfaatkan hanya untuk mengakses situs yang berkaitan dengan tugas dan pekerjaan guna kepentingan dinas;

b. Pengguna *Web Browsing* dilarang untuk :

1) Mengakses situs dengan konten pornografi, *adult materials*, *proxy avoidance*, *Mal*ware, *spyware*, *virus*, *Trojan Horse*, *Worm*, *phising*, dan situs yang dapat membahayakan keamanan komputer dan jaringan;

2) Mengunduh *file* dengan konten multimedia, *disc image*, dan yang tidak berhubungan dengan kepentingan dinas;

3) Menggunakan *browsing tools* atau *software* yang dapat mengganggu keamanan komputer dan jaringan;

4) Menggunakan *browsing tools* atau *software* yang dapat mengganggu kenyamanan Pengguna lain;

5) Menggunakan *tools* atau *software* untuk melakukan kecurangan (mengakses situs yang dilarang untuk diakses);

6) Mengakses situs yang memiliki *Digital Certificate* yang meragukan, misalnya tidak valid.

c. Pada jam kerja, Pengguna dilarang untuk mengakses situs dengan kategori :

Drug abuse, *occult*, *illegal or unethical*, *racism and hate*, *violence*, *marijuana*, *folklore*, *plagiarism*, *child abuse*, *abortion*, *gambling*, *extremist groups*, *nudity and risque*, *tasteless*, *alcohol*, *tobacco*, *lingerie and swimsuit*, *sports hunting and war games*, *advertising*, *brokerage and trading*, *freeware downloads*, *games*, *digital postcards*, *potentially bandwidth consuming* (*peer-to-peer file sharing*, *personal storage*, *multimedia download*, *internet radio and TV*, *internet telephony*), *arts and*

entertainment, *homosexuality*, *personal relationships*, *shopping and auction*, *society and lifestyles*, *real estate*, dan *business*;

d. Apabila terdapat tugas dan pekerjaan yang berkaitan dengan dinas untuk mengakses situs dengan kategori atau konten yang dilarang untuk diakses, harus mendapat persetujuan Penanggung Jawab dan berkoordinasi dengan Pengelola.

4. Pemanfaatan *Chatting*

Ketentuan dan Larangan

a. *Chatting* dimanfaatkan oleh Pengguna hanya untuk tugas dan pekerjaan yang berkaitan dengan kepentingan dinas;
b. Pengguna dilarang *Chatting* dengan *public chat server* selama jam kerja;
c. Hanya aplikasi *Chatting* yang ditentukan oleh Penanggung Jawab yang dapat digunakan;
d. Apabila terdapat tugas dan pekerjaan yang berkaitan dengan dinas dan mengharuskan untuk menggunakan *public chat server*, harus mendapat persetujuan tertulis Penanggung Jawab dan berkoordinasi dengan Pengelola.

5. Pemanfaatan VoIP

Ketentuan dan Larangan

a. Pemanfaatan VoIP hanya untuk tugas dan pekerjaan yang berkaitan dengan kepentingan dinas dan dilakukan selama jam kerja;
b. Hanya aplikasi atau *hardware* VoIP yang ditentukan oleh Lemsaneg yang dapat digunakan;
c. Apabila terdapat tugas dan pekerjaan yang berkaitan dengan dinas dan mengharuskan untuk menggunakan aplikasi atau *hardware* VoIP lain, maka harus mendapat persetujuan tertulis Penanggung Jawab dan berkoordinasi dengan Pengelola.

BAB III
ASPEK KEAMANAN TEKNOLOGI INFORMASI

A. Pengamanan Data dan Informasi

1. Pengendalian Akses Aplikasi, Data dan Informasi (Mengamankan Data dan Informasi dari Akses yang tidak ter-otorisasi)

a. Setiap akses terhadap aplikasi, data dan informasi di lingkungan Lemsaneg harus atas persetujuan Penanggung Jawab;
b. Setiap akses terhadap aplikasi, data dan informasi dengan menggunakan fasilitas pribadi harus teridentifikasi;
c. Setiap akses terhadap aplikasi, data dan informasi, termasuk akses tidak sah, dicatat sesuai dengan format dan bentuk yang ditentukan;
d. Menggunakan *access login* untuk membatasi akses terhadap aplikasi;
e. Fasilitas pengamanan harus dapat :
    1) Mengontrol Pengguna dalam mengakses aplikasi, data dan informasi;
    2) Mencegah sistem lain yang berusaha untuk melakukan akses ilegal terhadap aplikasi, data dan informasi;
f. *Remote access* hanya dapat dilakukan oleh pengguna yang telah diberikan otorisasi dan harus menggunakan pengamanan yang memadai melalui teknik identifikasi, otentikasi dan enkripsi.

2. Pengklasifikasian Data dan Informasi

a. Semua data dan informasi harus diklasifikasikan sesuai dengan nilai, tingkat sensitifitas, tingkat kekritisan dan tingkat kerahasiaannya oleh pemilik data dan informasi;
b. Klasifikasi data dan informasi berdasarkan nilai kerahasiaannya dibagi menjadi:
    1) Data dan informasi rahasia;
    2) Data dan informasi biasa;
c. Untuk data dan informasi yang bersifat rahasia harus disimpan di tempat khusus yang pengamanannya sesuai dengan standar yang berlaku;
d. Proses Re-Klasifikasi dilakukan dalam periode waktu tertentu sesuai dengan perubahan kebijakan yang berlaku atau perubahan nilai dari data dan informasi tersebut.

3. Pengelolaan Data dan Informasi

a. Administrasi Sistem

1) Proses pengelolaan dan perawatan data dan informasi yang terdapat pada server jaringan Lemsaneg hanya dilakukan oleh Pengelola;
2) Akses dan penggunaan data pada server jaringan Lemsaneg oleh Pengguna harus atas persetujuan Pengelola.

b. Pertukaran Data dan Informasi

Seluruh pertukaran data dan informasi yang berada di lingkungan Lemsaneg dilakukan dengan menggunakan fasilitas yang telah disediakan Pengelola Jaringan. Pertukaran data dan informasi menggunakan media penyimpanan tidak diperkenankan. Data dan informasi yang berada di lingkungan Lemsaneg tidak diperkenankan dibawa keluar lingkungan Lemsaneg dengan cara apapun.

c. Penyandian

1) Khusus penggunaan data dan informasi berklasifikasi rahasia, data *password/privacy* dan hal-hal lain yang berkaitan dengan pekerjaan di lingkungan Lemsaneg harus menggunakan sistem penyandian sesuai dengan standar yang sudah ditetapkan;
2) Pengelola menyarankan penggunaan perangkat dan/atau aplikasi enkripsi standar yang ditetapkan oleh Lemsaneg untuk mengenkripsi data dan informasi yang akan disimpan, ditransmisikan melalui jaringan internal, internet, *public network* maupun *wireless devices*;
3) Sistem penyandian yang dipakai meliputi aspek-aspek: *Integrity, Authentication, Availability* dan *non-repudiation*.

d. Penggunaan Aplikasi

1) Aplikasi yang digunakan di lingkungan Lemsaneg, baik di Server maupun *client* harus asli*;*
2) Pengunaan aplikasi pada Server jaringan Lemsaneg merupakan wewenang Pengelola;
3) Proses instalasi aplikasi pada sistem yang terhubung dengan jaringan komputer Lemsaneg harus atas persetujuan Pengelola.

e. Pengelolaan Data dan Informasi Dalam Media Penyimpanan

Tidak diperkenankan menggunakan media penyimpanan kecuali yang telah ditetapkan oleh Pengelola Jaringan.

B. Pengamanan Fisik

1. *Data Center* (Ruang Server)

a. Pembatasan akses masuk ke dalam ruang Server dengan menggunakan *secure door*, *RF ID card*, *pin* atau *password* dan *monitor surveillance;*

b. Menjaga kebersihan dengan tidak membawa makanan, minuman dan merokok di dalam ruang Server;

c. Menjaga temperatur ruangan (AC) sesuai dengan temperatur yang dianjurkan oleh pabrikan Server;

d. Pengaman dari bahaya bencana seperti kebakaran, gempa, banjir, huru-hara (*force majeur*);

e. Meletakkan atau menggunakan Alat Pemadam Api Ringan (APAR) yang aman bagi peralatan elektronik;

f. Menghindari pemakaian benda yang mudah terbakar di dalam atau di sekitar ruang Server.

2. *Power Supply*

a. *Power supply* utama yang berasal dari PLN harus melewati *Main Control Board* (MCB) khusus yang dapat dimatikan secara terpusat bila terjadi konsleting;

b. *Power supply* yang dipakai untuk Server dan komputer yang ada di dalam ruang Server harus menggunakan *Uninterrupted Power Supply* (UPS);

c. *Back up power supply* dengan genset atau *generator* di set agar waktu alih penggunaan *power supply* tidak menyebabkan Server atau peralatan elektronik yang berada di dalam ruang Server tidak mati;

d. Hindari pemakaian kabel gulung di dalam ruang server. Bila membutuhkan kabel tambahan karena keperluan tertentu harus mengunakan kabel tambahan yang aman dari kemungkinan konsleting.

3. Infrastruktur Jaringan

a. Kabel jaringan

1) Kabel jaringan harus terpasang dengan baik di dalam plafon atau kabel rel;

2) Penempatan kabel harus terlindung dari kemungkinan konsleting atau interfensi antara kabel LAN dengan sistem lain (PLN, Sistem Sensor, dan lain-lain);

3) Kabel LAN yang tidak terpakai harus di non aktifkan, baik dengan mencabut dari jaringan (*unplug*) atau tidak diberi layanan (*routing*).

b. *Switch* dan *Router*

1) Pemasangan *Switch* atau *Router* aman dari kemungkinan ancaman perusakan atau hilang;
2) Harus dalam kondisi ter-*password* dan terkunci agar tidak dapat di akses oleh pihak yang tidak berkepentingan.

c. Outlet LAN
1) Outlet LAN harus dalam keadaan terawat dan dapat digunakan dengan baik;
2) Pemasangan outlet harus ditempatkan di ruangan kerja, bukan di tempat umum yang sangat sulit dipantau;
3) Bila ada outlet yang terpasang di tempat pertemuan atau ruang tunggu harus dalam keadaan mati, bila ada tamu atau pihak lain yang tidak mempunyai akses ingin terkoneksi dengan LAN maka harus mendapat ijin dari Pengelola.

C. Pengamanan Jaringan

1. Pengamanan Server

a. Pengelolaan Server
a). Dilarang melakukan instalasi aplikasi pribadi atau yang tidak berhubungan dengan kebutuhan Server;
b). Akses jarak jauh terhadap Server harus dilakukan melalui jalur yang aman;
c). *Remote access* hanya dilakukan dalam lingkup terbatas (pembatasan akses dan *syntax*).

b. Kebijakan Konektivitas

2. Pengamanan c*lient*

a. Setiap c*lient* yang terhubung dalam jaringan harus terdata dengan baik oleh Pengelola (*hardware (Mac Address)* dan Penggunanya *(user id)*);
b. Setiap pengguna komputer *client* hanya boleh *login* sebagai Pengguna di dalam komputernya;
c. *Login admin* hanya dipergunakan oleh Pengelola dalam rangka pengembangan atau pemeliharaan sistem;
d. Setiap komputer milik pribadi yang terhubung dengan jaringan harus mendapat legitimasi dari Pengelola;
e. Pengaman fisik setiap *client* sepenuhnya menjadi tanggung jawab Pengguna;
f. Setiap *client* yang terhubung dengan LAN harus bebas dengan *virus, Trojan Horse, Malware;*

g. *Password* untuk *user login* dan *admin login* harus di *renewal* setiap bulan sekali dengan menggunakan minimal 8 karakter random (huruf, angka dan kapital);
h. Setiap *client* harus memiliki antivirus dan *Firewall* yang terinstal dan selalu dalam keadaan *up to date*;
i. Setiap selesai penggunaan, komputer harus dimatikan (*shutdown*) dan untuk laptop atau netbook disimpan ditempat yang aman dan terkunci.

3. *Virus, Trojan Horse, Malware*

a. Seluruh komputer inventaris Lemsaneg harus menggunakan program anti-virus yang ditentukan oleh Pengelola Jaringan;
b. Program anti-virus harus selalu *up-to-date* sekurang-kurangnya sekali dalam satu bulan;
c. Pengelola Jaringan harus menyediakan *update* program anti-virus *software server* untuk kepentingan pengguna secara umum;
d. Pengelola Jaringan harus melakukan pembersihan dengan segera apabila terdapat *public server* dalam jaringan terinfeksi oleh *virus atau Trojan Horse* atau *Malware* agar tidak menyebar lebih jauh ke dalam jaringan. Apabila proses pembersihannya memakan waktu yang relatif lama, maka Pengelola Jaringan akan memutuskan koneksi Server tersebut ke dalam jaringan;
e. Pengelola Jaringan berhak melakukan pemblokiran akses komputer ke dalam jaringan jika terdapat komputer yang diketahui terinfeksi *virus atau Trojan Horse* atau *Malware*, Pengguna harus segera melakukan upaya pembersihan, pemulihan dan pemeliharaan. Akses komputer ke dalam jaringan akan kembali dibuka setelah komputer dinyatakan bersih dari *virus* atau *Trojan Horse* atau *Malware* oleh Pengelola Jaringan;
f. Pengguna harus melakukan pemindaian terhadap komputernya masing-masing menggunakan program anti-virus yang *up-to-date* minimal 1 kali dalam sebulan.

4. Pemeriksaan Status Keamanan Jaringan

(1) Semua sistem yang aktif harus secara periodik dilakukan pemeriksaan rutin terhadap keamanannya, yaitu dengan melakukan pemindaian (*scanning*) terhadap kelemahan dalam semua *layer* (*7 layers Open System Interconnection*) yang ada;
(2) Apabila terjadi pelanggaran-pelanggaran terhadap keamanan jaringan, maka pemulihannya harus mengikuti standar baku dari Pengelola Jaringan;

(3) Penggunaan peralatan dan aplikasi keamanan untuk memeriksa status jaringan, disesuaikan keperluannya, sesuai persetujuan Penanggung Jawab dan koordinasi dengan Pengelola;
(4) Pengelola Jaringan harus membuat *review* tentang definisi dan kondisi keamanan jaringan secara rutin dan sistematik;
(5) Pengelola Jaringan dan Tim Audit TI Lemsaneg dapat memeriksa semua *record* yang tersimpan guna pemeriksaan rutin. Dan juga melakukan audit terhadap hasil forensik dan/atau melakukan audit karena penyalahgunaan wewenang.

5. Proses Pemeriksaan Keamanan Jaringan

a. Proses pemeriksaan harus mengacu pada rutinitas, yaitu:
   1) Setiap 6 bulan sekali, untuk sistem yang terkait langsung dengan internet dan sistem perimeternya;
   2) Setiap 6 bulan sekali, untuk sistem intranet dan Server yang berada di dalamnya;
   3) Setiap 12 bulan sekali, untuk semua komputer yang berada di dalam jaringan.
b. Semua proses harus dipastikan bahwa:
   1) Semua mandat dalam sistem pengaksesan adalah dalam koordinasi dengan Pengelola Jaringan;
   2) Hanya individu yang disetujui memegang Administrasi Keamanan Jaringan dan Sistem Otorisasi oleh Pengelola Jaringan sesuai standar yang sudah disepakati;
   3) Penggunaan aplikasi dan/atau skrip untuk tujuan pemantauan keamanan jaringan harus disupervisi oleh Pengelola Jaringan dan dicatat *file log*-nya.

6. *Review* keamanan jaringan

a. *Review* dimaksud untuk kegunaan verifikasi, bahwa semua proses yang ada dalam jaringan, hanya untuk mendukung proses kerja kedinasan Lemsaneg.
b. Semua hasil *review* disediakan sebagai bahan audit oleh Tim Audit TI Lemsaneg.
c. Tim Audit TI harus independen dari sistem yang mempengaruhinya.
d. Semua kelemahan hasil pemindaian pada semua *layer* terkait, harus segera dibuatkan tahapan-tahapan mekanisme pemantauan, pencegahan, pemulihan dan pemeliharaan.

   Objek yang terkait adalah:
   1) Perimeter.
   2) Akses internet.
   3) Manajemen Keamanan Jaringan.

4) Jasa Pelayanan Jaringan.
5) *Customization* aplikasi dan skrip.
6) Perangkat *Firewall* dan DMZ.
7) Pelayanan Intranet.
8) Server dan *Peripheral*.
9) OS.
10) *Database* dan aplikasi.
11) Dokumentasi.
12) Dan hal-hal lain yang patut ditambahkan.

D. Pengamanan OS

1. OS yang digunakan di lingkungan Lemsaneg, baik di Server maupun *client* harus memiliki lisensi yang sah, baik yang *shareware* maupun *freeware*.
2. OS dan aplikasi lainnya yang digunakan di setiap komputer harus selalu *up-to-date*, terutama untuk *security update* dari *web site* resmi.
3. *Backup System* dilakukan setidaknya satu kali dan disimpan oleh Pengelola Jaringan ataupun Pengguna terkait.
4. Kontrol Akses OS
   a. Setiap OS yang digunakan pada *hardware* milik Lemsaneg harus memiliki kontrol akses.
   b. Kontrol akses terhadap OS sekurang-kurangnya menggunakan *password* dengan standar yang ditentukan oleh Pengelola Jaringan.

E. Pengamanan Sumber Daya Manusia (SDM)

1. Pembuatan, penggantian dan pencabutan hak akses
   Hanya Pengelola dan Penanggung Jawab sistem TI yang berhak menentukan akses Pengguna terhadap sistem tersebut.
2. Peraturan dan tanggung jawab Pengguna
   a. Mematuhi segala peraturan yang berhubungan dengan SI dan TI Lemsaneg;
   b. Melindungi aset TI dari pihak yang tidak berkepentingan;
   c. Melaporkan kepada Pengelola apabila terjadi ancaman terhadap SI dan TI Lemsaneg;
   d. Tidak membocorkan *password;*
   e. Tidak memberitahukan informasi yang berkaitan dengan sistem keamanan yang digunakan pada SI dan TI Lemsaneg kepada pihak yang tidak berkepentingan.
3. Aset TI

a. Pengguna yang mendapatkan fasilitas TI karena jabatannya atau tugasnya bertanggung jawab terhadap aset TI tersebut.
b. Pengguna tidak diperbolehkan mengubah konfigurasi/OS dari fasilitas TI yang menjadi tanggung jawabnya kecuali berhubungan dan diperlukan untuk mendukung tugas dinas.
c. Pengguna yang karena sesuatu hal menyebabkan tidak berhak menggunakan fasilitas TI yang sebelumnya diberikan kepadanya, harus memberikan aksesnya terhadap fasilitas TI tersebut kepada Pengelola TI.

KEPALA LEMBAGA SANDI NEGARA
REPUBLIK INDONESIA,

WIRJONO BUDIHARSO