WALIKOTA YOGYAKARTA

PERATURAN WALIKOTA YOGYAKARTA

NOMOR 28 TAHUN 2008

TENTANG

STANDAR OPERASIONAL DAN PROSEDUR MANAJEMEN PENGAMANAN INFORMASI DIGITAL DAN PERANGKAT TELEKOMUNIKASI PADA PEMERINTAH KOTA YOGYAKARTA

WALIKOTA YOGYAKARTA,

Menimbang :

a. bahwa dalam rangka meningkatkan layanan e-government di lingkungan Pemerintah Kota Yogyakarta dalam bidang pengelolaan dan penyediaan informasi digital dan sarana telekomunikasi, maka perlu adanya standar operasional dan prosedur manajemen pengamanan informasi digital dan perangkat telekomunikasi di lingkungan Pemerintah Kota Yogyakarta;

b. bahwa untuk melaksanakan maksud tersebut diatas, maka perlu ditetapkan dengan Peraturan Walikota Yogyakarta.

Mengingat :

1. Undang-undang Nomor 16 Tahun 1950 tentang Pembentukan Daerah-daerah Kota Besar Dalam Lingkungan Propinsi Jawa Timur, Jawa Tengah, Jawa Barat dan Dalam Daerah Istimewa Yogyakarta;
2. Undang-undang Nomor 8 Tahun 1974 tentang Pokok-pokok Kepegawaian sebagaimana telah diubah dengan Undang-undang Nomor 43 Tahun 1999;
3. Undang-undang Nomor 32 Tahun 2004 tentang Pemerintahan Daerah, sebagaimana telah diubah beberapa kali yang terakhir dengan Undang-undang Nomor 12 Tahun 2008;
4. Peraturan Pemerintah Nomor 38 Tahun 2007 tentang Pembagian Urusan Pemerintahan antara Pemerintah, Pemerintahan Daerah Provinsi, dan Pemerintahan Daerah Kabupaten/Kota;

5. Keputusan Menteri Dalam Negeri Nomor 45 Tahun 1992 tentang Pokok-pokok Kebijaksanaan Sistem Informasi Manajemen Departemen Dalam Negeri (SIMDAGRI);
6. Peraturan Daerah Kotamadya Daerah Tingkat II Yogyakarta Nomor 1 Tahun 1992 tentang Yogyakarta Berhati Nyaman;
7. Peraturan Walikota Yogyakarta Nomor 68 Tahun 2007 tentang Standar Operasional Dan Prosedur Manajemen Client pada Pemerintah Kota Yogyakarta;
8. Peraturan Walikota Yogyakarta Nomor 72 Tahun 2007 tentang Standar Operasional Dan Prosedur Manajemen Pengamanan Jaringan Komputer pada Pemerintah Kota Yogyakarta;
9. Peraturan Walikota Yogyakarta Nomor 73 Tahun 2007 tentang Standar Operasional Dan Prosedur Manazjemen Server pada Pemerintah Kota Yogyakarta;
10. Peraturan Daerah Kota Yogyakarta Nomor 1 Tahun 2008 tentang Anggaran Pendapatan dan Belanja Daerah Tahun Anggaran 2008;
11. Peraturan Walikota Yogyakarta Nomor 10 Tahun 2008 tentang Penjabaran Anggaran Pendapatan dan Belanja Daerah Tahun Anggaran 2008.

MEMUTUSKAN :

Menetapkan : PERATURAN WALIKOTA YOGYAKARTA TENTANG STANDAR OPERASIONAL DAN PROSEDUR MANAJEMEN PENGAMANAN INFORMASI DIGITAL DAN PERANGKAT TELEKOMUNIKASI PADA PEMERINTAH KOTA YOGYAKARTA

Pasal 1

Dalam Peraturan Walikota ini yang dimaksud dengan :

1. Pemerintah Daerah adalah Pemerintah Kota Yogyakarta.
2. Walikota adalah Walikota Yogyakarta.
3. Satuan Kerja Perangkat Daerah yang selanjutnya disingkat SKPD adalah perangkat daerah pada Pemerintah Daerah selaku pengguna/pengelola informasi digital dan perangkat telekomunikasi.
4. Informasi digital yang selanjutnya disebut Informasi adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta,

rancangan, foto, *electronic data interchange* (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

5. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan atau menyebarkan informasi.
6. Telekomunikasi adalah setiap pemancaran, pengiriman dan atau penerimaan dari setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara dan bunyi melalui sistem kawat, optik, radio atau sistem elektromagnetik lainnya.
7. Alat telekomunikasi adalah setiap alat dan atau perlengkapan yang digunakan dalam bertelekomunikasi.
8. Perangkat telekomunikasi adalah sekelompok alat komunikasi yang memungkinkan dilakukannya telekomunikasi.

Pasal 2

Standar operasional dan prosedur manajemen pengaman informasi digital dan perangkat telekomunikasi pada Pemerintah Kota Yogyakarta sebagaimana tersebut dalam Lampiran Peraturan ini.

Pasal 3

Peraturan Walikota ini mulai berlaku pada saat diundangkan.

Agar supaya setiap orang mengetahuinya, memerintahkan pengundangan Peraturan ini dengan penempatannya dalam Berita Daerah Kota Yogyakarta.

Ditetapkan di Yogyakarta
pada tanggal 11 Juni 2008

WALIKOTA YOGYAKARTA

ttd

H. HERRY ZUDIANTO

Diundangkan di Yogyakarta
Pada tanggal 11 Juni 2008

SEKRETARIS DAERAH
KOTA YOGYAKARTA

ttd

H. RAPINGUN

BERITA DAERAH KOTA YOGYAKARTA TAHUN 2008 NOMOR 32 SERI D

LAMPIRAN : PERATURAN WALIKOTA YOGYAKARTA
NOMOR : 28 TAHUN 2008
TANGGAL :11 Juni 2008

STANDAR OPERASIONAL DAN PROSEDUR MANAJEMEN PENGAMANAN INFORMASI DIGITAL DAN PERANGKAT TELEKOMUNIKASI PADA PEMERINTAH KOTA YOGYAKARTA

A. Daftar Istilah

1. *Removable media* adalah alat penyimpanan data komputer yang tidak terpasang secara permanen pada komputer sehingga mudah untuk dibawa dan dipindahkan dari satu komputer ke komputer lain.
2. *Firewall* adalah kombinasi perangkat keras dan perangkat lunak yang digunakan untuk membatasi akses menuju dan atau dari suatu jaringan komputer.
3. *Peak load testing* atau pengujian beban puncak adalah pengujian yang dilakukan terhadap sistem informasi dengan melakukan simulasi permintaan akses oleh banyak pengguna untuk mengetahui apakah sistem informasi tersebut mampu melayani permintaan sesuai dengan yang diperkirakan.
4. *Stress testing* adalah pengujian yang dilakukan untuk mengetahui stabilitas sistem informasi jika menerima akses pengguna yang melebihi rata-rata.
5. Memori *volatile* adalah memori yang akan kehilangan data jika tidak ada arus listrik.
6. *Cookies* adalah informasi yang disimpan dalam komputer pengguna oleh web browser ketika mengakses suatu website yang dapat digunakan untuk mengenali kembali pengguna yang bersangkutan ketika melakukan akses berikutnya.
7. *File attachment* adalah file yang ikut disertakan dalam sebuah email sebagai lampiran.
8. *Social engineering* adalah teknik yang digunakan seseorang yang tidak berhak untuk memperoleh hak akses terhadap suatu sistem komputer dari orang yang berhak melalui telpon, email, tatap muka, dan sebagainya.
9. *File sharing* adalah tindakan yang dilakukan sehingga file yang terdapat dalam sebuah komputer dapat diakses dari komputer lain.
10. *Stabilizer* listrik adalah alat yang digunakan untuk menjaga stabilitas tegangan listrik.
11. UPS atau *Uninterruptible Power Supply* adalah alat yang digunakan untuk menjaga ketersediaan pasokan listrik ketika pasokan dari sumber utama mengalami kegagalan.

12. *System Administrator* adalah orang yang bertanggung jawab terhadap perencanaan, pengaturan dan pemeliharaan sistem komputer atau jaringan komputer sehigga dapat digunakan dengan baik oleh pengguna.
13. *Remote Management* adalah fitur yang memungkinkan seseorang untuk melakukan kendali dan penyesuaian pengaturan dari lokasi manapun.
14. *Remote Access* adalah kemampuan untuk mengakses komputer dari jarak jauh.
15. Kabel Tanah *Duct* adalah kabel yang dilindungi oleh pelindung dari bahan tertentu sebelum ditanam dalam tanah.
16. Kabel Atas Tanah adalah kabel yang dibentangkan diatas permukaan tanah.

B. Pedoman Umum

1. Pengamanan informasi digital di lingkungan Pemerintah Daerah mengacu kepada pedoman standar pengamanan informasi *International Standards Organisation 17799* yang dipublikasikan oleh *International Organization for Standardization*.
2. Penggunaan perangkat teknologi informasi yang portable (mudah dibawa) di lingkungan Pemerintah Daerah dibatasi dengan aturan-aturan untuk mencegah terjadinya kebocoran informasi sensitif milik Pemerintah Daerah.
3. Akses terhadap informasi milik Pemerintah Daerah diatur dengan *access control* untuk mencegah terjadinya akses ilegal dan penyalahgunaan informasi yang merugikan kepentingan pemerintah dan masyarakat.
4. Perlindungan terhadap aset informasi milik Pemerintah Daerah dilakukan dengan memperhatikan asas :
    a. *confidentiality* (Kerahasiaan) yang menjamin bahwa informasi hanya dapat diakses oleh yang berwenang;
    b. *integrity* (integritas) yang menjamin bahwa informasi hanya dapat diubah oleh yang berwenang;
    c. *availability* (ketersediaan) yang menjamin bahwa informasi dapat selalu tersedia untuk diakses oleh yang berwenang.
5. Pemerintah Daerah menugaskan dan memberikan pelatihan kepada beberapa karyawannya agar memiliki kualifikasi cukup untuk mengelola perangkat teknologi informasi dan komunikasi baik perangkat keras maupun perangkat lunak.
6. Semua karyawan Pemerintah Daerah memiliki tanggung jawab untuk ikut serta melindungi dan memelihara keamanan informasi dan perangkat telekomunikasi milik Pemerintah Daerah.

7. Karyawan Pemerintah Daerah yang diberi tugas dan tanggung jawab untuk mengelola informasi dan perangkat telekomunikasi milik Pemerintah Daerah wajib melakukan *backup* secara berkala untuk menjaga keberlangsungan operasional perangkat teknologi informasi dan telekomunikasi jika terjadi kerusakan maupun bencana.
8. Setiap perangkat teknologi informasi dan komunikasi milik Pemerintah Daerah memiliki dokumentasi serta petunjuk operasional yang memadai.

C. Maksud dan Tujuan

Maksud dan tujuan diterbitkannya Standar Operasional dan Prosedur Manajemen Pengamanan Informasi Digital dan Perangkat Telekomunikasi pada Pemerintah Daerah adalah untuk dijadikan pedoman dan acuan oleh setiap SKPD di Pemerintah Daerah dalam menggunakan dan mengelola informasi digital dan perangkat telekomunikasi untuk mendukung pelaksanaan E-Government yang efektif dan efisien dalam rangka meningkatkan pelayanan kepada masyarakat umum.

D. Ruang Lingkup

Ruang lingkup Pedoman Standar Operasional dan Prosedur Manajemen Pengamanan Informasi Digital dan Perangkat Telekomunikasi pada Pemerintah Daerah adalah untuk :

1. penggunaan perangkat keras dan perangkat lunak;
2. pengaturan hak akses terhadap informasi;
3. pengelolaan sumber daya manusia;
4. pengelolaan informasi dan dokumen;
5. pengelolaan sarana dan prasarana telekomunikasi.

E. Perangkat Keras dan Komponennya

1. Hanya karyawan Pemerintah Daerah yang boleh menggunakan *removable media* untuk melakukan transfer data dari dan ke dalam perangkat teknologi informasi Pemerintah Daerah.
2. Pekerjaan perbaikan dan pemeliharaan perangkat keras yang tidak dilakukan sendiri oleh Pemerintah Daerah hanya boleh diserahkan kepada pihak ketiga (rekanan) yang sudah ditunjuk secara resmi oleh Pemerintah Daerah.
3. Penggunaan komputer portable (laptop) sebagai komputer kerja oleh karyawan Pemerintah Daerah harus atas sepengetahuan pejabat yang berwenang.

4. Karyawan Pemerintah Daerah yang menggunakan komputer portable (laptop) sebagai komputer kerja bertangungjawab atas kerahasiaan informasi milik Pemerintah Daerah yang terdapat dalam perangkat tersebut.
5. Pemindahan perangkat keras milik Pemerintah Daerah ke lokasi di luar lingkungan Pemerintah Daerah harus mendapat ijin dan atau pengawasan dari pejabat yang berwenang atau karyawan Pemerintah Daerah yang diberi wewenang.
6. *Removable media* yang berisi informasi penting dan rahasia harus disimpan dalam tempat penyimpanan yang aman dan terkunci serta tahan api.
7. Semua perangkat penyimpanan data digital milik Pemerintah Daerah hanya boleh dimusnahkan atas ijin dari pejabat yang berwenang.
8. Karyawan Pemerintah Daerah yang bekerja dengan komputer harus memastikan bahwa layar komputer kerja dalam keadaan kosong dan terkunci ketika ditinggalkan.

F. Pengendalian Akses Terhadap Informasi

1. Semua sistem informasi milik Pemerintah Daerah harus memiliki fitur *access control* yang mampu melakukan pembatasan akses informasi oleh pengguna yang mana pengelompokan pengguna ditentukan oleh kebijakan Pemerintah Daerah.
2. Semua sistem informasi milik Pemerintah Daerah harus dilengkapi dengan fitur yang mengharuskan user untuk menggunakan *password* yang panjangnya minimal 8 (delapan) karakter.
3. Akses terhadap sistem informasi dan dokumen milik Pemerintah Daerah hanya boleh dilakukan oleh pengguna yang diberi wewenang.
4. Instalasi dan modifikasi perangkat lunak yang terdapat pada komputer milik Pemerintah Daerah hanya boleh dilakukan oleh petugas yang berwenang atau oleh pihak lain atas seijin Pemerintah Daerah dan pengaturannya merujuk kepada SOP manajemen *client* Pemerintah Daerah.
5. Semua karyawan Pemerintah Daerah yang memiliki akses terhadap sistem informasi milik Pemerintah Daerah wajib menjaga kerahasiaan akun dan *password* yang dipercayakan kepadanya.
6. Semua karyawan Pemerintah Daerah yang memiliki akses terhadap sistem informasi milik Pemerintah Daerah wajib melakukan perubahan *password* secara berkala.
7. Akses fisik terhadap komputer milik Pemerintah Daerah hanya boleh dilakukan oleh karyawan Pemerintah Daerah.

8. Akses terhadap sistem informasi Pemerintah Daerah harus dicatat dalam *file log* dan dimonitor untuk mendeteksi terjadinya penyalahgunaan sistem informasi serta untuk evaluasi terhadap kebijakan pengelompokan *access control*.
9. Karyawan Pemerintah Daerah yang ketugasannya sudah tidak lagi menggunakan suatu sistem informasi harus segera dihapus akunnya dari sistem informasi tersebut.
10. Akses internet dari dalam jaringan komputer Pemerintah Daerah diatur dengan perangkat yang dapat melakukan filterisasi terhadap informasi yang dilarang oleh Pemerintah Daerah.
11. Akses internet dari dan ke jaringan komputer Pemerintah Daerah dibatasi dengan *firewall* yang pengaturannya merujuk kepada SOP manajemen jaringan Pemerintah Daerah.
12. *Remote access* kedalam jaringan komputer Pemerintah Daerah hanya boleh dilakukan oleh karyawan Pemerintah Daerah yang diberi wewenang dan atas sepengetahuan pejabat yang berwenang.
13. *Remote management* terhadap perangkat jaringan dan server oleh *system administrator* tidak boleh dilakukan dari sembarang komputer dan pengaturannya merujuk kepada SOP manjemen server Pemerintah Daerah.
14. Komputer milik Pemerintah Daerah yang fungsi utamanya adalah untuk mengakses sistem informasi yang berhubungan dengan pelayanan masyarakat tidak diperbolehkan untuk mengakses dan mengambil file dari internet.

G. Pemrosesan Informasi dan Dokumen

1. Pemerintah Daerah menugaskan berapa karyawannya sebagai *system administrator* yang bertanggungjawab untuk memelihara perangkat keras dan perangkat lunak teknologi informasi dan komunikasi.
2. Komputer milik Pemerintah Daerah yang fungsi utamanya adalah untuk mengakses sistem informasi yang berhubungan dengan pelayanan masyarakat harus dilengkapi dengan antivirus.
3. Pendistribusian informasi milik Pemerintah Daerah dalam bentuk file harus atas sepengetahuan pejabat yang berwenang.
4. Pendistribusian informasi yang bersifat rahasia harus dilindungi dengan enkripsi dan *digital signature.*
5. File yang berasal dari *email attachment* tidak boleh dibuka sebelum discan dengan antivirus.
6. Karyawan Pemerintah Daerah yang memiliki akun email di server mail Pemerintah Daerah wajib menjaga agar akunnya tidak mengalami *overquota*.

7. Karyawan Pemerintah Daerah yang menerima *email* dari pihak ketiga dan dicurigai sebagai *email* sampah tidak diperkenankan untuk membuka email tersebut.
8. Pemerintah Daerah menugaskan beberapa karyawannya untuk bertanggungjawab dan melakukan pemeliharaan terhadap informasi yang ditampilkan dalam situs resmi Pemerintah Daerah.
9. File yang tidak dikenal asal-usulnya tidak boleh dibuka dengan komputer milik Pemerintah Daerah.
10. Pemerintah Daerah menugaskan beberapa karyawannya untuk bertanggungjawab dan melakukan pemeliharaan terhadap database milik Pemerintah Daerah.
11. Modifikasi terhadap database yang tidak melalui aplikasi sistem informasi harus atas sepengetahuan pejabat yang berwenang.
12. *Removable media* di lingkungan Pemerintah Daerah hanya boleh digunakan oleh karyawan yang diberi ijin dan atas sepengetahuan pejabat yang berwenang.
13. Informasi yang disimpan dalam sistem informasi milik Pemerintah Daerah memiliki retensi yang sesuai dengan pedoman kearsipan pada Pemerintah Daerah.
14. Pembuatan database baru harus melalui pengecekan untuk memastikan bahwa dapat bekerja dengan baik sebelum digunakan untuk menyimpan data yang sesungguhnya dan digunakan dalam operasional.
15. File harus disimpan dengan nama yang mencerminkan isi file.
16. Klasifikasi kerahasiaan dan kepemilikan dokumen harus dicantumkan dalam *header* atau *footer* dokumen tersebut.
17. *Recycle bin* dan file temporer dalam komputer milik Pemerintah Daerah harus dihapus setidaknya 1 (satu) minggu sekali.
18. Karyawan Pemerintah Daerah yang bekerja menggunakan komputer PC dan laptop harus melakukan *back up* secara berkala terhadap *file* kerjanya.
19. *System administrator* yang bertanggungjawab terhadap database harus melakukan *backup* secara berkala dalam *removable media* dan *storage server*.
20. *System administrator* yang bertanggungjawab terhadap database harus melakukan pengujian terhadap *backup* database dan memastikan bahwa *backup* tersebut tidak cacat.
21. Karyawan Pemerintah Daerah yang sehari-harinya bekerja dengan *file* harus melakukan *backup* terhadap *file* kerjanya secara berkala dalam *removable media*.

22. *Backup* dalam *removable media* harus dienkripsi dan disimpan di tempat yang aman dan terpercaya di luar gedung milik Pemerintah Daerah seperti misalnya *safe deposit box* di bank.
23. Semua informasi digital yang dialihmediakan kedalam bentuk cetakan (*hardcopy*) untuk diberikan kepada pihak ketiga harus atas sepengetahuan pejabat yang berwenang.
24. *File* yang berisi informasi rahasia harus dilindungi dengan *password* dan disimpan dalam format yang tidak dapat diubah tanpa kewenangan yang cukup.
25. Tanggungjawab pengelolaan data dan informasi yang dikategorikan sensitif oleh Pemerintah Daerah harus ditangani oleh 2 (dua) orang karyawan dan perubahan yang dilakukan oleh salah satunya harus diketahui oleh yang lain.

H. Pengadaan Sistem Informasi

1. Pembuatan sistem informasi yang tidak dilakukan secara swadaya oleh Pemerintah Daerah hanya boleh diserahkan kepada pihak ketiga (rekanan) yang sudah ditunjuk secara resmi oleh Pemerintah Daerah atau Pemerintah Pusat.
2. Kode sumber yang terdapat pada semua sistem informasi yang dibuat untuk Pemerintah Daerah tidak boleh diberikan kepada pihak lain.
3. Sistem Informasi yang dibuat untuk Pemerintah Daerah harus mengalami pengujian dan dinyatakan lulus oleh pejabat yang berwenang sebelum digunakan dalam operasional sehari-hari di lingkungan Pemerintah Daerah.
4. Pengujian terhadap sistem informasi baru yang menggunakan data riil milik Pemerintah Daerah harus dilakukan dengan pengawasan oleh karyawan Pemerintah Daerah yang ditunjuk oleh pejabat yang berwenang.
5. Pengujian terhadap sistem informasi untuk Pemerintah Daerah meliputi *peak loading* dan *stress testing*.
6. Sebelum suatu sistem informasi Pemerintah Daerah digunakan, akun dan *password* yang dipakai untuk pengujian harus dihapus.
7. Sebelum digunakan sepenuhnya, sistem informasi yang mengalami peremajaan maupun sistem informasi baru yang tujuannya untuk menggantikan sistem informasi yang sudah ada, harus digunakan secara paralel dengan sistem informasi yang sudah ada hingga dinyatakan sempurna oleh pejabat yang berwenang.
8. Sistem Informasi yang dibuat untuk Pemerintah Daerah harus dirancang agar tidak menampilkan pesan kesalahan yang dapat memperlihatkan desain dan konfigurasi sistem informasi tersebut.

9. Sistem informasi yang menangani data dan informasi yang dikategorikan sensitif dan rahasia oleh Pemerintah Daerah harus mampu melakukan enkripsi jika data dan informasi tersebut mengalami kondisi-kondisi sebagai berikut :
    a. tersimpan dalam file atau database;
    b. tersimpan dalam *registry* sistem operasi;
    c. tersimpan dalam memori *volatile;*
    d. terkirim ke komputer lain;
    e. tersimpan sebagai *cookies.*
10. Sistem informasi yang mengalami peremajaan maupun sistem informasi baru harus memiliki dokumentasi penggunaan dan pemeliharaan teknis.

I. Manajemen Sumber Daya Manusia

1. *System administrator* secara berkala mendapatkan pelatihan untuk meningkatkan pengetahuan dan kemampuan sesuai dengan bidang yang ditanganinya.
2. Pelatihan harus diberikan kepada karyawan Pemerintah Daerah yang akan menggunakan dan melakukan pemeliharaan teknis terhadap sistem informasi yang baru.
3. Karyawan Pemerintah Daerah yang sehari-harinya bekerja dengan perangkat teknologi informasi secara berkala mendapatkan pelatihan mengenai pemahaman terhadap keamanan informasi yang meliputi antara lain :
    a. pemahaman agar mampu mengamankan laptop dan informasi yang terdapat di dalamnya;
    b. pemahaman agar tidak meggunakan *password* yang berkaitan dengan data pribadi;
    c. pemahaman agar tidak menyimpan *password* di sembarang tempat;
    d. pengetahuan tentang informasi yang dianggap sensitif dan harus dijaga kerahasiaannya;
    e. pengetahuan tentang bahaya yang dapat ditimbulkan oleh *file attachment* dalam *email* yang dikirimkan oleh pihak yang tidak dikenal;
    f. pemahaman agar mampu mengindari ancaman keamanan dari *social engineering*;
    g. pengetahuan tentang bahaya yang dapat ditimbulkan oleh instalasi perangkat lunak yang tidak dikenal pada komputer kerja;
    h. pengetahuan tentang bahaya yang dapat ditimbulkan dengan mengaktifkan *file sharing* pada komputer kerja tanpa seijin *system administrator.*

4. Karyawan Pemerintah Daerah yang sehari-harinya bekerja dengan perangkat teknologi informasi milik Pemerintah Daerah tidak diperbolehkan melakukan perubahan terhadap konfigurasi perangkat lunak baik sistem operasi maupun program aplikasi yang terdapat pada komputer kerjanya.
5. Tindakan yang harus dilakukan oleh karyawan Pemerintah Daerah dalam menangani dan merespon insiden yang mengancam keamanan informasi antara lain :
   a. mengisolir komputer yang dicurigai mengalami masalah dengan memutus kabel jaringan dan tidak melakukan *copy* data dari atau ke komputer tersebut melalui media apa pun.
   b. segera melaporkannya pada *system administrator*.

J. Perangkat Telekomunikasi

1. Pengkondisian, perlakuan dan pemeliharaan PABX (sentral mini) milik Pemerintah Daerah harus memperhatikan hal-hal sebagai berikut :
   a. lokasi instalasi harus bebas dari kemungkinan ancaman bahaya banjir, kebocoran, lembab, debu dan gempa.
   b. lokasi instalasi harus dilengkapi dengan alat yang dapat mengatur kelembaban dan suhu udara yang besarannya disesuaikan dengan petunjuk pengaturan kelembaban dan suhu udara pada buku manual PABX.
   c. penyaluran listrik untuk perangkat PABX milik Pemerintah Daerah harus melalui *stabilizer* listrik dan UPS.
   d. penyaluran listrik untuk perangkat PABX milik Pemerintah Daerah harus memiliki *backup* dari generator listrik.
   e. penyaluran listrik untuk perangkat PABX harus memiliki *grounding* yang besarannya kurang dari 3 (tiga) Ohm.
   f. pemerintah Daerah menunjuk beberapa karyawannya untuk menjadi pengelola PABX.
   g. akses untuk mengatur perangkat PABX milik Pemerintah Daerah dilindungi dengan *password* yang hanya boleh diketahui oleh pengelola PABX.
   h. karyawan Pemerintah Daerah yang diberi tugas untuk mengelola PABX wajib untuk menjaga kerahasiaan *password* PABX.
   i. pekerjaan perbaikan dan pemeliharaan perangkat PABX yang tidak dilakukan oleh pengelola PABX Pemerintah Daerah hanya boleh dilakukan oleh pihak ketiga (rekanan) yang ditunjuk secara resmi oleh Pemerintah Daerah.
   j. pekerjaan perbaikan dan pemeliharaan perangkat PABX oleh pihak ketiga (rekanan) harus didampingi oleh pengelola PABX Pemerintah Daerah.

k. setelah pekerjaan perbaikan dan pemeliharaan perangkat PABX selesai dilakukan oleh pihak ketiga, pengelola PABX Pemerintah Daerah harus segera melakukan penggantian *password* PABX.

l. pengelola PABX Pemerintah Daerah wajib melakukan pemeriksaan dan pembersihan fisik terhadap perangkat PABX milik Pemerintah Daerah setidaknya 1 (satu) minggu 1 (satu) kali untuk memastikan bahwa perangkat PABX bebas dari debu, serangga dan binatang lainnya.

2. Pengkondisian, perlakuan dan pemeliharaan Terminal Pembagi Utama (MDF) milik Pemerintah Daerah harus memperhatikan hal-hal sebagai berikut :

a. MDF dilindungi dalam sebuah kotak yang terbuat dari bahan kedap air dan mempunyai ventilasi cukup agar tidak lembab, bebas dari semut dan binatang lainnya;

b. setiap terminal terminasi dilengkapi dengan arrestor yang berfungsi sebagai penyalur arus lebih yang melewati urat kabel (distribusi) langsung ke sistem *grounding*;

c. tata cara penataan terminal dalam perangkat PABX milik Pemerintah Daerah harus mengikuti kaidah yang berlaku, sehingga memudahkan pekerjaan *jumpering* dan peletakan *jumper wire* dilakukan dengan rapi;

d. suplai listrik untuk perangkat MDF milik Pemerintah Daerah harus memiliki *grounding* yang besarannya kurang dari 3 (tiga) Ohm;

e. setiap *screen cable* / *alluminium foil* dari setiap kabel (distribusi atau PABX) harus dihubungkan dengan bar *grounding* secara individual;

f. terminal MDF yang digunakan adalah jenis tekan sisip dan diberi label;

g. semua pekerjaan terhadap terminal MDF harus selalu menggunakan alat *insertion tools* yang sesuai dengan jenis terminal dan dilarang menggunakan obeng minus untuk melakukan *jumpering*;

h. diameter *jumper wire* disamakan dengan diameter kabel distribusi dan PABX;

i. pekerjaan *jumpering* dilakukan dengan prinsip jalur terpendek dan dilakukan dengan rapi serta selalu disisakan alokasi klem terminal cadangan.

3. Pengkondisian, perlakuan dan pemeliharaan kabel distribusi perangkat telekomunikasi milik Pemerintah Daerah harus memperhatikan hal-hal sebagai berikut :

a. pemasangan kabel distribusi perangkat telekomunikasi milik Pemerintah Daerah menggunakan kombinasi antara kabel tanah *duct* dan kabel atas tanah;

b. tiang untuk kabel atas tanah menggunakan tiang besi atau tiang beton dengan tinggi kabel 6 meter dari permukaan tanah;

c. tiang besi harus dicor dengan kedalaman 30 (tiga puluh) centimeter dan ketinggian 30 (tiga puluh) centimeter dari permukaan tanah dan harus dicat;

d. jika rute kabel atas tanah saling berpotongan dengan kabel listik, maka sudut perpotongan adalah 45 (empat puluh lima) sampai dengan 90 (sembilan puluh) derajat, dan jarak antar kabel tergantung tegangan kabel listrik sebagai berikut :
   1) 0,6 meter untuk tegangan kabel listrik 650 V;
   2) 1,2 meter untuk tegangan kabel listrik 11 kV;
   3) 2,1 meter untuk tegangan kabel listrik 66 kV;
   4) 3 meter untuk tegangan kabel listrik 132 kV;
   5) 3,6 meter untuk tegangan kabel listrik 220 kV.

e. jika rute kabel atas tanah saling sejajar dengan kabel listik, maka jarak antar kabel tergantung tegangan kabel listrik sebagai berikut :
   1) 1,2 meter untuk tegangan kabel listrik 650V;
   2) 3,5 meter untuk tegangan kabel listrik diatas 650V.

4. Pengkondisian, perlakuan dan pemeliharaan titik distribusi perangkat telekomunikasi milik Pemerintah Daerah harus memperhatikan hal-hal sebagai berikut :
   a. terminal titik distribusi dilindungi pada suatu kotak yang kedap terhadap air, mempunyai ventilasi cukup agar tidak lembab, bebas dari semut dan binatang lainnya;
   b. terminal terminasi dilengkapi dengan arrestor yang berfungsi sebagai penyalur arus lebih langsung ke sistem *grounding*;
   c. lokasi penempatan titik distribusi harus diupayakan ditengah-tengah area layanan, sehingga panjang kabel instalasi ke terminal pengguna tidak lebih dari 250 (dua ratus lima puluh) meter, aman dari kemungkinan gangguan, aksebilitas mudah, dan estetis;
   d. pekerjaan *jumpering* di terminal titik distribusi harus menggunakan *insertion tools* yang sesuai.
5. Untuk mempermudah penanganan gangguan, perencanaan kedepan dan integrasi dengan sistem lain maka sistem pendokumentasian perangkat telekomunikasi di Pemerintah Daerah harus memperhatikan hal-hal sebagai berikut :
   a. nomor telepon (extension), nama dan alamat pengguna, fitur atau fasilitas yang ada, tanggal instalasi, catuan titik distribusi, nama kabel distribusi, urat kabel distribusi, nomor terminal MDF.
   b. nama titik distribusi, urat kabel distribusi, kapasitas titik distribusi, isi nomor telepon dan tanggal instalasi, status sisa kapasitas (baik, rusak atau cadangan) dan tanggal validasi.
   c. dibuatkan peta jaringan yang terdiri dari skema kabel dan lokasi.

6. Tower milik Pemerintah Daerah yang digunakan untuk instalasi perangkat repeater harus dilengkapi dengan penangkal petir dan sistem *grounding* yang memadai.
7. Semua panggilan telepon keluar menuju nomer yang bukan milik Pemerintah Daerah harus melalui operator.
8. Semua panggilan telepon ke nomer ekstension Pemerintah Daerah harus melalui operator.
9. Semua nomer ekstension yang melakukan panggilan keluar menuju nomer yang bukan milik Pemerintah Daerah harus direkam dalam *billing system* milik Pemerintah Daerah.

WALIKOTA YOGYAKARTA

ttd

H. HERRY ZUDIANTO