WALIKOTA YOGYAKARTA

PERATURAN WALIKOTA YOGYAKARTA

NOMOR 76 TAHUN 2007

TENTANG

STANDAR OPERASIONAL DAN PROSEDUR MANAJEMEN
PENGAMAN SISTEM INFORMASI DAN KOMUNIKASI
PADA PEMERINTAH KOTA YOGYAKARTA

WALIKOTA YOGYAKARTA,

Menimbang : a. Bahwa dalam rangka meningkatkan layanan e-Government Pemerintah Kota Yogyakarta dalam bidang informasi dan telekomunikasi maka perlu adanya standar operasional dan prosedur manajemen pengaman sistem informasi dan telekomunikasi di lingkungan Pemerintah Kota Yogyakarta;

b. bahwa untuk melaksanakan maksud tersebut di atas 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 dengan Undang-undang Nomor 8 Tahun 2005;

4. Peraturan Pemerintah Nomor 41 Tahun 2007 tentang Organisasi Perangkat Daerah;

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 Daerah Kota Yogyakarta Nomor 23 Tahun 2005 tentang Pembentukan, Susunan Organisasi dan Tata Kerja Badan Informasi Daerah;

8. Peraturan Daerah Kota Yogyakarta Nomor 3 Tahun 2007 tentang Anggaran Pendapatan dan Belanja Daerah Tahun Anggaran 2007;

9. Peraturan Walikota Yogyakarta Nomor 34 Tahun 2007 tentang Penjabaran Anggaran Pendapatan dan Belanja Daerah Tahun Anggaran 2007;

MEMUTUSKAN :

Menetapkan : PERATURAN WALIKOTA YOGYAKARTA TENTANG STANDAR OPERASIONAL PROSEDUR MANAJEMEN PENGAMAN SISTEM INFORMASI DAN KOMUNIKASI PADA PEMERINTAH KOTA YOGYAKARTA.

BAB I
KETENTUAN UMUM
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 atau yang selanjutnya disebut SKPD adalah perangkat daerah pada Pemerintah Daerah selaku pengguna/pengelola server.

4. Sistem adalah sebagai kumpulan dan komponen yang saling berkaitan untuk secara bersama-sama menghasilkan satu tujuan.

5. Manajemen adalah berkaitan dengan pembagian tanggung jawab, yang menjamin tidak akan terjadinya tumpang tindih pekerjaan. Sedangkan administrasi berkaitan dengan sistem pencatatan pada setiap penanggung jawab serta pelaporan antar penanggungjawab yang telah ditetapkan dalam manajemen tersebut.

6. Pengamanan secara umum dapat didefinisikan sebagai bebas dan bahaya atau dalam kondisi selamat, Secara spesifik dalam keamanan komputer didefinisikan sebagai perlindungan data dan computer.

7. Prosedur adalah rangkaian langkah atau kegiatan yang saling berhubungan satu sama lain secara esensial yang diikuti pendekatan fungsional

BAB II
STANDAR OPERASIONAL DAN PROSEDUR
Pasal 2

Standar Operasional dan Prosedur Manajemen Pengaman Sistem Informasi dan Komunikasi pada Pemerintah Kota

Yogyakarta adalah sebagaimana lersebut dalam Lampiran Peraturan ini.

Pasal 3

Peraturan ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Yogyakarta
pada tanggal 11 Desember 2007

WALIKOTA YOGYAKARTA

ttd

H. HERRY ZUDIANTO

Diundangkan di Yogyakarta
pada tanggal 11 Desember 2007

SEKRETARIS DAERAH
KOTA YOGYAKARTA

ttd

Drs. RAPINGUN
NIP.490017536

BERITA DAERAH KOTA YOGYAKARTA TAHUN 2007 NOMOR ..84. SERI D

LAMPIRAN : PERATURAN WALIKOTA YOGYAKARTA
NOMOR : 76 TAHUN 2007
TANGGAL : 11 DESEMBER 2007

STANDAR OPERASIONAL DAN PROSEDUR MANAJEMEN PENGAMAN SISTEMINFORMASI DAN KOMUNIKASI PADA PEMERINTAH KOTA YOGYAKARTA

A. Pedoman Umum

1. Manajemen Pengaman Sistem Informasi dan Telekomunikasi pada Pemerintah Kota Yogyakarta harus memperhatikan aspek kerahasiaan data agar terhidar dari penerobosan akses, penyadapan data dan penipuan (social engineering).

2. Manajemen Pengaman Sistem Informasi dan Telekomunikasi pada Pemerintah Kota Yogyakarta harus memperhatikan aspek integritas data dan menjamin bahwa data yang dimiliki hanya dapat diubah oleh yang berwenang.

3. Manajemen Pengaman Sistem Informasi dan Telekomunikasi pada Pemerintah Kota Yogyakarta harus dapat menjamin ketersediaan layanan yang kontinyu bagi masyarakat.

4. Manajemen Pengaman Sistem Informasi dan Telekomunikasi pada Pemerintah Kota Yogyakarta harus memperhatikan aspek-aspek yang dapat meningkatkan kesadaran pengguna akan pentingnya keamanan dalam menggunakan teknologi informasi.

5. Manajemen Pengaman Sistem Informasi dan Telekomunikasi pada Pemerintah Kota Yogyakarta harus memperhatikan aspek-aspek untuk meningkatkan keamanan dalam pengelola sisem informasi dan komunikasi di lingkungan Pemerintah Kota Yogyakarta dengan mempertimbangkan:

   a. Asas manfaat
      Mampu dimanfaatkan seoptimal mungkin dan dapat menyajikan informasi yang bermanfaat memperlancar pelaksanaan tugas.

   b. Asas Keamanan dan Keandalan
      Menjamin keamanan serta keadaan informasi yang diolah ,disimpan,dan disajikan

   c. Asas Efektif dan Efisien
      Menunjang keberhasilan pelaksanaan tugas, baik tugas pokok maupun tugas penunjang secara efektif,(selesai tepat waktu) dan efisien (hemat dalam pengguanaan sumber daya)

   d. Asas keterpaduan
      Merupakan satu kesatuan / keterpaduan dari berbagai kepentingan secara serasi dan proposional

   e. Asas integrasi
      Mampu memadukan /mempersatukan semua informasi strategis sebagai bahan pertimbangan dalam keputusan bagi pimpinan.

f. Asas Otorisasi
Pemilikan dan penyajian informasi harus sesuai dengan kewenangan masing-masing dan peraturan perundang-undangan yang berlaku.

B. Maksud dan Tujuan

Maksud dan tujuan diterbitkannya Standar Operasional dan Prosedur Manajemen Pengaman Manajemen Pengaman Sistem Informasi dan Telekomunikasi pada Pemerintah Kota Yogyakarta adalah untuk dijadikan pedoman dan acuan oleh setiap Satuan Kerja Perangkat Daerah (SKPD) di Pemerintah Kota Yogyakarta dalam mengelola dan menggunakan perangkat dan sistem yang terkait dengan teknologi informasi dan komunikasi agar dapat meningkatkan pelayanan kepada masyarakat umum.

C. Ruang Lingkup

Ruang lingkup Standar Operasional dan Prosedur Manajemen Pengaman Sistem Informasi dan Telekomunikasi pada Pemerintah Kota Yogyakarta adalah untuk :
1. Perangkat keras pendukung teknologi informasi dan komunikasi;
2. Perangkat lunak pendukung teknologi informasi dan komunikasi;
3. Sumber daya manusia dibidang teknologi informasi dan komunikasi;

D. Pokok-pokok keamanan

Pokok-pokok keamanan informasi mencakup dua area yaitu (1) keamanan informasi secara fisik dan (2) keamanan informasi secara logika. Yang mana pada dasarnya terfokuskan pada dua hal yaitu (1) otentikasi dan (2) otorisasi.

1. Keamanan informasi secara fisik

Keamanan informasi secara fisik dapat diartikan sebagai upaya perlindungan terhadap sistem organisasi/instansi dari serangan secara fisik, yang meliputi semua elemen fisik sistem yaitu :
   a. Melindungi mesin dimana aplikasi dijalankan;
   b. Melindungi ruangan dimana mesin tersebut dioperasikan;
   c. Melindungi gedung dimana mesin tersebut diinstal; dan
   d. Melindungi daerah tempat dimana perusahaan berada.

Elemen-elemen fisik tersebut harus dijaga dan dilindungi dari segala macam gangguan dan ancaman yang mungkin dapat terjadi.
Keamanan informasi secara fisik juga termasuk mengamankan saluran komunikasi, baik komunikasi melalui kabel ataupun melalui gelombang *(wireless).* Dimana jaringan komunikasi harus terlindung dari usaha penyadapan dan kerusakan, seperti misalnya terputusnya kabel.

2. Keamanan informasi secara logika

Keamanan informasi secara logika dihubungkan pada solusi masalah-masalah keamanan TI berupa arsitektur TI, aplikasi dan proses. Jaringan komunikasi harus dilindungi dengan baik tidak saja secara fisik namun juga secara logika. Sebab saat ini hampir semua organisasi/institusi dan individu terhubung ke jaringan umum internet.

Dengan terhubung ke internet maka sumberdaya di dalam komputer kita juga akan terhubung dan dapat diakses dari jauh. Karena itu sangat diperlukan perlindungan terhadap data/informasi yang penting dan sensitif yang dimiliki, agar tidak dapat diakses oleh pihak-pihak yang tidak berhak.

Perlindungan tersebut harus diterapkan di berbagai tingkatan keamanan. Dan perlindungan itu juga harus mencakup dari mulai mendesain aplikasi, membuat alur prosesnya hingga sistem penyimpanannya. Desain keamanan informasi pun

perlu dibuat sedemikian rupa sehingga dapat menutup celah keamanan yang diketemukan.

E. Kebijakan dan regulasi keamanan informasi

Kebijakan keamanan informasi dapat mendefinisikan proses-proses yang terjadi pada area yang berbeda didalam organisasi. Serta berfokus pada keamanan antar proses, misalnya bagaimana meminta password baru, menganti dll.

Kebijakan keamanan informasi pada dasarnya terfokuskan pada dua hal yaitu otentikasi dan otorisasi.

a. Otentikasi

Yang dimaksud otentikasi dalam TI adalah proses mengkonfirmasi keabsahan seseorang/sesuatu *(user)* tersebut benar sesuai dengan yang terdapat dalam *database.* Kebijakan otentikasi ini akan dapat mengendalikan *user* terhadap penggunaan sumberdaya sistem dan untuk menghindari pemalsuan identitas.

Proses otentikasi meliputi pengumpulan informasi yang unik dari para *user* dan kemudian disimpan dalam sebuah *database.* Terdapat tiga mekanisme pengumpulan informasi untuk otentikasi yaitu (1) basis pengetahuan, seperti *username* dan *password;* (2) basis kunci, seperti anak kunci (pintu), kunci algoritma sandi dan *smartcard;* (3) basis biometrik, seperti sidik jari, pola suara, dan DNA.

Dalam prakteknya mekanisme pengumpulan informasi untuk otentikasi ini sering dikombinasikan untuk mendapatkan hasil otentikasi yang lebih baik. Sebagai contoh sertifikat digital yang merupakan gabungan basis pengetahuan dengan kunci, atau *voice password* yang merupakan gabungan basis pengetahuan dengan biometrik.

Jenis Otorisasi :

1) *Username* dan *password* adalah metode otentikasi yang paling terkenal. *User* yang akan mengakses ke sistem diminta mengetikkan *username* dan *password* untuk dicocokkan dengan *database* sistem.

2) Kunci (fisik) adalah sebuah objek yang dapat digunakan untuk membuktikan identitas pemegangnya. Biasanya terbuat dari logam untuk mengunci komputer atau dapat juga berupa sebuah peralatan *hardware* yang dihubungkan dengan computer untuk mengaktifkan program aplikasi. Atau dapat juga berupa sebuah *smartcard.*

3) Otentikasi biometrik adalah penggunaan ciri-ciri fisik atau karakteristik tubuh sebagai sarana pencocokan identitas yang diterjemahkan kedalam sebuah nilai digital dan kemudian disimpan dalam sistem. Saat ini otentikasi biometrik telah semakin populer digunakan.

b. Otorisasi

Otorisasi adalah sebuah proses pengecekan kewenangan *user* dalam mengakses sumberdaya yang diminta. Terdapat dua metode dasar Otorisasi yaitu (1) daftar pembatasan akses dan (2) daftar kemampuan.

1) Daftar pembatasan akses *(access control list)* umumnya berisi daftar *users* dengan masing-masing tugasnya/kewenangannya terhadap sumberdaya sistem, misalnya *use, read, write, execute, delete* atau *create.* Secara spesifik merupakan aturan yang memberikan jenis kewenangan kepada *users* atas sumberdaya sistem.
2) Daftar kemampuan *(capability list)* hampir sama dengan daftar pembatasan akses, namun dengan pendekatan yang berbeda yaitu dengan penitik beratan pada tugas/kewenangan.

Pada kenyataannya daftar pembatasan akses lebih sering digunakan karena mengelola jenis Otorisasi ini relatif lebih mudah.
Tugas/kewenangan masing-masing tingkat keamanan secara spesifik berbeda, mengakibatkan berbeda *user* berbeda pula tugas/kewenangan sehingga pembatasan akses selalu mengacu pada tugas/kewenangan yang menyertainya.

F. Komunikasi yang aman

Komunikasi yang aman dimaksudkan untuk melindungi data/informasi ketika sedang ditransmisikan dari upaya penyadapan, manipulasi atau perusakan. Teknik pengamanan data/informasi tersebut secara umum biasanya menggunakan teknik penyandian/kriptografi.

Komunikasi yang aman selalu berlandaskan kesaling pengertian (dalam otentikasi dan Otorisasi) antara pengirim dan penerima yang biasa dikenal dengan istilah *handshake* atau kontrak. Untuk membangun saling pengertian tersebut, maka diperlukan sebuah menejemen kunci atau manajemen keamanan informasi. Keamanan dalam arti proses serta hasil pelayanan dapat memberikan keamanan dan kenyamanan serta dapat mem-berikan kepastian hukum. Keamanan informasi adalah topik yang sangat luas dan kompleks, namun secara singkat keamanan informasi meliputi ;

1. Otentikasi, yaitu proses mengkonfirmasi keabsahan seseorang sebelum diijinkan mengakses informasi dalam sistem.

2. Pembatasan akses, yaitu membatasi jumlah dan jenis informasi yang boleh diperoleh oleh seseorang dari sistem.

3. Kerahasiaan, yaitu melindungi informasi dalam sistem agar hanya dapat diakses oleh pihak-pihak yang berhak saja.

4. Intergritas data, yaitu melindungi data dari perubahan-perubahan yang tidak dikehendaki baik secara sengaja ataupun tidak sengaja.

5. *Non-repudiation* atau tidak dapat disangkal, yaitu berarti bahwa seseorang yang telah melakukan transaksi dalam sistem tidak dapat menyangkal aktifitas tersebut.

6. Kebijakan, yaitu keputusan-keputusan yang mengikat bagi pengguna sistem.

7. Ketersediaan, yaitu jaminan bahwa sistem dapat selalu diakses oleh pengguna.

8. Kriptografi, yaitu teknik yang digunakan untuk mengacak informasi dengan tata cara dan kunci tertentu agar tidak terbaca oleh pihak yang tidak berhak.

G. Organisasi pengelolaan sistem informasi manajemen

Organisasi pengelolaan sistem informasi manajeman harus memiliki kemampuan seperti apa yang telah ditetapkan di dalam pengertian sistem informasi manajemen, baik dari segi fisik maupun fungsinya.
Sehubungan dengan itu, maka organisasi pengelolaan sistem informasi harus menggambarkan secara fungsional tugas-tugas yang berkenaan dengan pengembangan, pemeliharaan dan pengoperasiannya. Fungsi-fungsi dan bentuk dasar dari organisasi pengelolaan sistem informasi manajemen adalah sbb:

1) Analisa sistem, merupakan proses mendefinisikan dan menggambarkan kebutuhan pemakai secara detail yang meliputi penetapan ruang lingkup sistem dan pengumpulan fakta.

2) *Administrator,* adalah pengguna komputer yang mempunyai hak akses penuh melakukan perubahan terhadap konfigurasi dari sistem maupun perangkat yang digunakan.
3) Pangkalan data atau basis data, merupakan suatu sistem penyimpanan data yang tersusun sedemikian rupa dalam bentuk elektronik.
4) Sistem operasi, merupakan suatu perangkat lunak yang bertugas untuk melakukan kontrol dan manajemen perangkat keras serta operasi-operasi dasar sistem komputer.
5) Pelatihan, merupakan usaha untuk meningkatkan kemampuan personil dalam hal penguasaan teknologi informasi.

Fungsi analisa sistem mempunyai tugas untuk merumuskan kebutuhan pengguna informasi dan merancang sistem yang memberikan jawaban atas kebutuhan tersebut. Administrator pangkalan data mempunyai tugas untuk melakukan penerapan dan pengontrolan terhadap definisi data maupun definisi hubungan antarfile data dan juga merancang sistem keamanan pangkalan data. Penyusunan program berperanan sebagai pembuat program aplikasi yang akan digunakan untuk proses dengan komputer
Sistem Informasi di Pemerintah Kota Jogjakarta meliputi dua jenis Sistem yang terdiri:

1. Sistem Informasi Layanan Masyarakat:
   a. Layanan berbasis Web
   b. Layanan berbasis SMS
   c. Layanan berbasis Telepon/Fax
   d. Layanan melalui Tatap Muka

2. Sistem Informasi Layanan Aparatur

   a. SIM KEPEGAWAIAN
   b. SIM BADA
   c. SIM GAJI
   d. SIM RETRIBUSI KEBERSIHA
   e. SIM ARSIP
   f. SIM KEPENDUDUKAN
   g. SIM HUKUM
   h. SIM SIUP
   i. SIM TDP
   j. SIM PERIZINAN
   k. SIM PENELITIAN
   l. SIM CAPIL
   m. SIM NAKERTRANS
   n. SIM REKLAME
   o. SIM PJU
   p. SIM IMBB
   q. SIM PENDIDIKAN
   r. SIM ASENERING
   s. SIM PASAR
   t. SIM PERENCANAAN
   u. SIM SM PENGENDALIAN
   v. SIM KEUANGAN DAERAH
   w. SIM INTEGRASI
   x. SIM PELAYANAN PUSKESMAS
   y. SIM UJI KENDARAAN BERMOTOR
   z. SIMPEMAKAMAN
   aa. SIM UKM
   bb. SIM PARIWISATA
   cc. SIM PUSKESMAS

H. Arab pengembangan SIM

Sesuai dengan dasar-dasar konsepsional yang telah diuraikan terdahulu maka pengembangan sistem informasi manajemen di lingkungan Pemerintah Kota Yogyakarta di arahkan pada:

1. Berkembanganya peranan informasi untuk mendukung aktivitas manajenal dalam fungsinya sebagai sumber daya manusia, setelah ketenagaan, keuangan dan sarana/prasarana

2. Terselenggaranya suatu sistem produksi dan pendayagunaan informasi dalam suatu siklus yang teratur dan berada dalam satu koordinasi pengelolaan yang berada di Badan Informasi Daerah Kota Yogyakarta.

3. Terwujudnya fungsi pengelolaan sistem informasi manajemen sebagai subsistem manajenal.

4. Terbinanya aktivitas manajerial di bidang perencanaan, administrasi pengelolaan, administrasi pemantauan, pengambilan keputusan dan statistik tahunan.

WALIKOTA YOGYAKARTA

ttd

H. HERRY ZUDIANTO