KEPUTUSAN
KEPALA BADAN PENGAWASAN KEUANGAN DAN PEMBANGUNAN
NOMOR : KEP-06.00.00-210/K/2002

TENTANG
KEBIJAKAN SISTEM DAN TEKNOLOGI INFORMASI
PADA BADAN PENGAWASAN KEUANGAN DAN PEMBANGUNAN

KEPALA BADAN PENGAWASAN KEUANGAN DAN PEMBANGUNAN,

Menimbang:
a. bahwa dalam rangka mendukung tercapainya visi dan misi serta menunjang kelancaran kegiatan operasional Badan Pengawasan Keuangan dan Pembangunan, diperlukan sistem dan teknologi informasi yang memadai, baik perangkat keras ataupun perangkat lunak dengan mempertimbangkan aspek manfaat, keamanan, dan efisiensi;
b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a perlu menetapkan Keputusan Kepala Badan Pengawasan Keuangan dan Pembangunan tentang Kebijakan Sistem dan Teknologi informasi Badan Pengawasan Keuangan dan Pembangunan.

Mengingat:
1. Keputusan Presiden Republik Indonesia Nomor 115/M Tahun 1999;
2. Keputusan Presiden Republik Indonesia Nomor Nomor 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi. Kewenangan. Susunan Organisasi dan Kerja Lembaga Pemerintah Non Departemen. sebagaimana telah diubah dengan Keputusan Presiden Republik lndonesia Nomor 3 Tahun 2002;
3. Keputusan Presiden Republik Indonesia Nomor 110 Tahun 2001 tentang Unit Organisasi dan Tugas Eselon I Lembaga Pemerintah Non Departemen sebagaimana telah diubah dengan Keputusan Presiden Nomor 5 Tahun 2002;
4. Keputusan Kepala Badan Pengawasan Keuangan dan Pembangunan Nomor: KEP-06.00.00-080/K/2001 tentang Organisasi dan Tata Kerja Badan Pengawasan Keuangan dan Pembangunan;
5. Keputusan Kepala Badan Pengawasan Keuangan dan Pembangunan Nomor: KEP-06.00.00-286/K/2001 tentang Organisasi dan Tata Kerja Perwakilan Badan Pengawasan Keuangan dan Pembangunan sebagaimana telah diubah dengan Keputusan Kepala Badan Pengawasan Keuangan dan Pembangunan Nomor: KEP-06.00.00-626/K/2001;
6. Keputusan Kepala Badan Pengawasan Keuangan dan Pembangunan Nomor: KEP-01.00.00-296/K/2001 tentang Perencanaan Strategis (Renstra) BPKP 2000-2004

MEMUTUSKAN:

Menetapkan :

PERTAMA : Kebijakan Sistem dan Teknologi Informasi Badan Pengawasan Keuangan dan Pembangunan sebagaimana tercantum dalam lampiran Keputusan ini.

KEDUA : Kebijakan Sistem dan Teknologi Informasi Badan Pengawasan Keuangan dan Pembangunan sebagaimana dimaksud dalam diktum PERTAMA digunakan sebagai landasan kegiatan operasional sehubungan pengelolaan perangkat keras *(hardware),* perangkat lunak *(software)* sumber daya manusia *(brainware)* teknologi informasi di lingkungan Badan Pengawasan Keuangan dan Pembangunan;

KETIGA : Kebijakan ini mencakup dan mengatur tentang : penggunaan

sistem dan internet; keamanan aset teknologi informasi; pengembanganperangkat lunak; pengelolaan pusat data; pengelolaan jaringan komputer baik di tingkat *Local Area Network* (LAN); *Metropolitan Area Network* (MAN) *Wide Area Network* (WAN); pengelolaan akses jaringan computer; investasi perangkat keras dan perangkat lunak; dan penanganan/penanggulangan bencana (*disaster recovery plan*);

KEEMPAT : Seluruh lingkup kegiatan di bidang sistem dan teknologi informasi sebagaimana dimaksud dalam diktum KEDUA dan KETIGA tersebut diatas, wajib dikoordinasikan dengan Pusat Informasi Pengawasan Badan Pengawasan Keuangan dan Pembangunan;

KELIMA : Keputusan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 17 April 2002
KEPALA BADAN PENGAWASAN KEUANGAN
DAN PEMBANGUNAN
ttd.
ARIE SOELENDRO

LAMPIRAN KEPUTUSAN KEPALA BADAN PENGAWASAN KEUANGAN DAN PEMBANGUNAN
NOMOR : KEP-06.00.00.210/K/2002
TANGGAL : 17 APRIL 2002

I. DEFINISI

Penuangan daftar definisi/istilah di bagian berikut ini dimaksudkan agar pembaca mendapatkan pemahaman, sudut pandang, atau persepsi yang sama dengan apa yang terkandung dalam surat keputusan ini. Daftar definisi/istilah tersebut disajikan urut abjad *(alphabethical)* sebagai berikut :

ISTILAH	DEFINISI
Administrator	Suatu fungsi yang ditunjuk oleh Kepala Pusinfowas untuk menyelenggarakan pencatatan atau pengadministrasian sesuai bidangnya. Terdiri dari antara lain: *Mail Adminitrator* bertugas mengadministrasikan surat-surat intern melalu intranet, dan *Web Administrator* bertugas mengelola web internet, serta *Database Administrator* bertugas mengelola *database, Network Administrator* bertuga mengelolajaringan komputer (suara dan data).
Application log	Catatan-catatan yang berkaitan dengan akses ke suatu aplikasi.
Arsitektur terbuka	Suatu kerangka jaringan yang bersifat dapat diakses oleh pihak lain.
Aset Teknologi	Asset (aktiva) yang berhubungan dengan instalasi sistem informasi mencakup : manusia *(knowledge),* perangkat keras, perangkat lunak sistem, perangkat lunak, aplikasi, file data/informasi, dokumentasi sistem, fasilitas dan alat pendukung lainnya.
Audit trail	Segalajenis catatan *(log),* atau tahapan/riwayat yang berkaitan dengan pencatatan dan pemrosesan suatu transaksi atau informasi tertentu, yang dimaksudkan agar pada suatu saat informasi tersebut dapat dilakukan pelacakan penelusuran kembali untuk tujuan tertentu misalnya audit.
Back up	1. Duplikasi data ke dalam bentuk atau media penyimpangan lainnya denban tujuan bila data originalnya tidak berfungsi (rusak) atau hilang, maka duplikasi ini diharapkan dapat menggantikannya; atau 2. Sistem dan prosedur yang digunakan untuk menggantikan teknologi informasi yang dipakai sehari-hari apabila karena sesuatu hal menjadi tidak berfungsi. Sistem dan prosedur *backup* tersebut meliputi perangkat keras, perangkat lunak, data/file dan sarana lainnya.
Backbone	Jalur utama yang membawa data dari kumpulan jalur-jalur yang lebih kecil yang bermuara kepadanya. Pada tingkat lokal, *backbone* dapat diartikan sebagai jalur dimana jaringan lokal menghubungkan diri ke jaringan luas atau MAN *(Metropolitan Area Network)*/WAN *(Wide Area Network).*
Bugs	Lubang kesalahan dalam program.

Bugs Fixes	Perbaikan kesalahan dalam suatu program.
Corrective maintenance	Suatu bentuk pemeliharaan untuk memperbaiki kesalahan yang sudah terjadi.
Data Center (Pusat Data*)*	Adalah tempat atau ruangan yang dirancang secara khusus untuk menyimpan, mengelola, dan mengoperasikan perangkat keras dan perangkat lunak pengelola data.
Data Communication (Komunikasi data)	Suatu metode transmisi data atau informasi melalui sarana telekomunikasi.
Data Owner (Pemilik Data)	Adalah pegawai maupun pejabat BPKP yang karena fungsi dan jabatannya bertanggung jawab atas semua data dan informasi yang dihasilkan serta dikelola dan/atau dikumpulkannya selama bekerja untuk dan atas nama instansinya.
Data sangat Rahasia, Rahasia, Terbatas/ Konfidensial, Biasa.	a. Sangat Rahasia (SR) : data yang informasinya membutuhkan tingkat pengamanan yang tertinggi. Tingkat pengamanan informasi surat (data) erat hubungannya dengan keamanan dan keselamatan negara serta hanya boleh diketahui oleh pejabat yang berhak menerimanya. b. Rahasia (R) : data yang informasinya membutuhkan tingkat pengamanan yang tinggi. Tingkat pengamanan informasi surat (data) erat hubungannya dengan keamanan kedinasan dan hanya boleh diketahui oleh pejabat yang berwenang atau yang ditunjuk. c. Terbatas/Konfidensial (K) : data yang informasinya membutuhkan tingkat pengamanan yang tinggi. Tingkat pengamanan informasi surat (data) erat hubungannya dengan tugas khusus kedinasan dan hanya boleh diketahui oleh pejabat yang berwenang atau yang ditunjuk. d. Biasa : data yang tidak memerlukan pengamanan khusus.
Decryption (dekripsi)	Adalah proses konversi terhadap data yang telah di-enkripsi ke dalam bentuk aslinya *(original),* sehingga data tersebut dapat dibaca dan dimengerti kembali oleh pembacanya.
Detective maintenance	Suatu bentuk pemeliharaan untuk mengetahui kesalahan sebelum terjadi.
Dial- up Line/*Switched Line*	Saluran telepon *(dial* atau *push button)* yang dapat digunakan sebagai media untuk mentrasmisikan data antar lokasi tertentu. Biaya pemakaian dihitung atau tergantung dari berapa lama saluran tersebut dipakai.
Direct Implentation	Implementasi suatu sistem yang dilaksanakan secara langsung mengganti sistem sebelumnya.
Disaster Recovery Plan	Adalah rencana pemulihan data dan sistem BPKP pada kondisi darurat, dimana sistem utama BPKP dan/atau perangkat pendukung sistem utama BPKP diperkirakan tidak dapat dipergunakan sebagai akibat adanya kerusakan sumber listrik, kerusakan sarana komunikasi dan jaringan komputer, kebakaran, banjir, bencana alam, sabotase / pelanggaran, atau kondisi darurat lain yang

	ditetapkan oleh Ketua Tim Pengenda1ian Keadaan Darurat BPKP.
E-Mail system	Adalah *electronic mail* melalui jaringan BPKP *(intranet)* dan/atau melalui jaringan publik (internet) untuk keperluan tukar menukar pesan atau informasi di lingkungan BPKP.
Encryption (Enkripsi)	Teknik yang digunakan untuk mengaburkan/menyamarkan data dengan tujuan untuk mengamankan data dan menyimpan kerahasiaan data tersebut, atau proses konversi data ke bentuk lain (biasa disebut sebagai *ciphertext*/teks yang teracak) yang sulit dimengerti oleh orang yang tidak berhak atas data tersebut.
End-User (Pengguna Akhir)	Orang atau pihak yang menggunakan sistem aplikasi yang ada di BPKP.
Freewvare	Perangkat lunak umum yang dapat dimiliki dan digunakan secara gratis *(r-ee on charge)* atau tanpa biaya.
Hak Akses Minimal	Tingkat akses yang dimiliki oleh pengguna sesuai dengan fungsi, penugasan, dan jabatannya.
Inhouse Development (Pengembangan intern)	Adalah pengembangan perangkat lunak yang pelaksanaannya dilakukan dengan menggunakan sistem dan sumber daya manusia internal BPKP (staf/pegawai sendiri).
Internet	Adalah suatu jaringan internasional yang menghubungkan seluruh jaringan-jaringan kecil melalui komputer-komputer yang ada di perusahaan-perusahaan, akademik, maupun kalangan publik/masyarakat di dunia yang memanfaatkan TCP / IP *net- work protocol.*
Intranet	Adalah suatu jaringan local/perusahaan *(corporate network)* yang menggunakan infrastruktur dan standar internet dan *the world wide web*. Dengan kata lain, intranet adalah jaringan komunikasi seperti internet tapi hanya dapat diakses dan hanya untuk kepentingan internal perusahaan.
Jaringan Telekomunikasi Data	Suatu jaringan telekomunikasi yang digunakan untuk melakukan transmisi data dari suatu lokasi ke lokasi lainnya.
Ketua Tim Pengendalian Keadaan Darurat BPKP	Petugas yang diangkat dengan Surat Keputusan Kepala BPKP mengenai pengendalian keadaan darurat dan bertugas/bertanggung jawab atas pengendalian keadaan darurat yang terjadi di BPKP.
Kompabilitas	Terjadi di mana suatu hardware/software bisa di jalankan dalam hardware/software lainnya.
Kondisi *disaster*	Kondisi dimana sistem utama BPKP dan atau perangkat pendukung sistem utama BPKP diperkirakan tidak dapat dipergunakan atau dioperasikan secara normal dalam 24 jam atau lebih yang dapat disebabkan oleh kerusakan sumber listrik, kerusakan sarana komunikasi dan jaringan komputer, kebakaran, banjir, gempa bumi, sabotase dan pelanggaran, atau kondisi darurat (bencana alam) lainnya yang ditetapkan oleh Ketua Tim Pengendalian Keadaan Darurat BPKP.

Konfigurasi Jaringan	Suatu kerangka dari jaringan.
Konfigurasi sistem	Suatu kerangka dari sebuah sistem.
Kustodi Data dan Sistem *(data dan system custodian)*	Adalah pihak yang diberi wewenang dan tanggung jawab oleh pemilik data *(Data Owner)* dalam hal ini adalah Pusinfowas, untuk melakukan pengelolaan dan penyimpanan data yang bertujuan menjamin ketersediaan data dan sistem.
Leased Line *(Dedicated Line)*	Saluran komunikasi data yang disewa secara khusus, misalnya saluran telepon, dengan pengenaan beban tetap (biaya tetap) dalam periode tertentu, yang biasanya per bulan (bulanan).
Libray and Librarian	Sistem Penyimpanan untuk dokumentasi seluruh kegiatan Teknologi Informasi.
Local Area Network (LAN)	Sistem komunikasi data setempat/lokal dalam bentuk jaringan komputer (misalnya terdiri dari beberapa *Personal Computer)* dalam suatu ruangan, gedung atau lokasi tertentu yang dihubungkan dengan saluran komunikasi secara khusus.
Logical access	Akses ke jaringan secara tidak kasat mata.
Metropolitan Area Network (MAN)	Jaringan komputer dan beberapa komputer atau LAN yang saling berhubunan satu sama lain, dimana jaringan komputer tersebut berada di berbagai tempat/gedung namun masih dalam satu kota yang sama. Misalnya, jaringan komputer di BPKP Pusat dengan jaringan komputer di BPKP Perwakilan DKI Jakarta I atau Puslitbang BPKP (masih dalam satu lokasi metropolitan, yaitu DKI Jakarta).
Mitra Kerja BPKP	Adalah pihak-pihak di luar BPKP yang bekerjasama dengan Pusinfowas.
Network Protocol	Suatu kerangka jaringan yang bersifat data diakses oleh pihak lain.
Open Architecture	Adalah arsitektur terbuka yang memungkinkan pihak lain untuk dapat secara mudah bekerjasama dengan perangkat lainnya sesuai dengan strandar internasional.
Open System	Adalah sistem terbuka yang memungkinkan sistem-sistem lain dapat secara mudah bekerjasama dengan sistem tersebut sesuai dengan strandar internasional.
Operating System (OS)	Adalah perangkat lunak yang harus ada dan selalu aktif karena berfungsi mengatur pelaksanaan operasional sistem komputer. Setiap *operating system* (OS) memiliki kemampuan berbeda tergantung ukuran serta kompleksitas sistem komputer yang dikontrolnya. Pada umumnya, OS terdiri dari *scheduling, input/output control, compilation, storage, assignment, data management* dan pelayanan rutin lainnya.
Otentikasi	Adalah proses untuk mengetahui apakah seseorang atau sesuatu adalah benar-benar sesuai dengan yang dinyatakan oleh orang atau sesuatu tersebut. Dalam jaringan internal ataupun jaringan publik (termasuk internet), otentikasi umumnya dilakukan dengan menggunakan *password logon.*

	Pengetahuan tentang *password* dianggap menjamin bahwa pengguna adalah otentikasi (benar sesuai dengan yang dinyatakan). Setiap pengguna pada awalnya mendaftarkan diri (atau didaftarkan oleh orang lain), dengan menggunakan *password* yang dipilih sendiri. Untuk setiap pemakaian, pengguna tersebut harus mengetahui dan menggunakan *password* yang telah terdaftar sebelumnya. Kelemahan sistem ini adalah pada penggunaan transaksi yang signifikan (seperti pemindahan uang, dsb) akibat *password* tercuri atau diketahui orang lain secara tidak sengaja, atau karena pemiliknya lupa.
Outsorcing Development (Pengembangan ekstern)	Adalah pengembangan perangkat lunak ataupun jasa pengelolaan sistem yang dilakukan oleh pihak ketiga (vendor konsultan, atau rekanan). Pihak ketiga ini harus secara resmi ditunjuk oleh BPKP.
Paches	Program yang dipergunakan untuk menutupi kesalahan dalam program lainnya.
Packet Switched Network	Merupakan suatu jaringan telekomunikasi digital yang pesana-pesannya dibagi ke dalam sejumlah blok transmisi data yang ditetapkan sesuai dengan kebutuhan jaringan transmisi.
Paralel run	Implementasi suatu sistem yang dilaksanakan secara simultan dengan sistem sebelumnya yang sudah ada.
Password	Suatu kode atau simbol khusus yang ada dalam sistem komputer sehingga orang yang akan mengakses (seperti mengakses data, program, ataupun aplikasi komputer) harus memiliki atau mengenal kode atau simbol *(password)* tersebut. *Password* digunakan untuk tujuan identifikasi dan pengamanan sistem komputer. Masing-masing pengguna diberi satu set karakter/*alphanumeric* untuk dapat mengakses seluruh atau sebagian sistem komputer.
(Private Branch eXchange) PBX	Sebuah sistem switching telepon internal yang digunakan untuk menghubungkan satu extension dengan extension lainnya maupun dengan jaring, telepon publik.
Pengamanan Fisik	Adalah suatu sistem pengamanan untuk mencegah akses oleh pihak-pihak yang tidak berwenang terhadap area komputerisasi serta peralatannya, yang meliputi peralatan mekanikal, elektronis, elektromekanika digital, sistem komputer ruang komputer, ruang terminal, fasilitas komunikasi data, dan *movement detection (detector, close circuit television camera, moitor, electronic eyes* atau *infra alarm,* dan sebagainya).
Pengamanan Logik	Suatu sistem pengamanan untuk mencegah akses oleh pihak-pihak yang tidak berwenang terhadap sistem komputer dan informasi yang tersimpan didalamnya. Sistem tersebut sekurang-kurangnya meliputi penggunaan *User Id, password* serta pembatasan akses terhadap "menu" sistem komputer dan program aplikasi yang tersimpan didalamnya.

Perangkat Keras *(Hardware)*	Peralatan fisik yang digunakan dalam media input, pemrosesan, maupun output data elektronis, seper1 keybord, mouse, monitor, *Central Procesing Unit* (CPU), printer, modem, dan sebagainya.
Perangkat Lunak *(Software)*	Sekumpulan program komputer yang berisikal serangkaian perintah untuk mengendalikan kegiatan suatu sistem komputer atau untuk mengoperasikan aplikasi.
Perangkat lunak Aplikasi *(Aplication Software)*	Suatu program komputer yang dibuat untuk melaksanakan tugas-tugas tertentu.
Perangkat Lunak Komunikasi Data *(Data Communication Software)*	Suatu program komputer yang dapat membatasi terminal-terminal komputer, dapat berhubungan dengan aplikasi tertentu, dan dapat mengontrol penggunaan enkripsi data.
Perangkat Lunak Pengaman *(Security System Software)*	Suatu program komputer yang melekat pada *Operaing System* (OS) perangkat lunak, dimana pengguna dalam mengoperasikan komputer disyaratkan harus memasukkan *User Id* dan *password,* yang tidak ditampakkan pada layar monitor, dan/atau suatu program komputer yang melekat pada perangkat lunak aplikasi yang bertujuan membatasi akses dari pengguna lainnya atas menu-menu tertentu yang telah ditetapkan.
Perangkat lunak Sistem *(System software)*	Suatu program komputer yang berhubungan dengan kontrol-kontrol terhadap perangkat keras komputer, untuk membantu *programmer* aplikasi dalam melakukan tugas-tugasnya, ataupun berhubungan dengan fungsi-fungsi lain yang tidak berkaitan dengan pengguna.
PIN *(Personal Identification Number)*	Suatu jaringan digit "unik" yang mengidentifikasi pengguna komputer dan dimaksudkan untuk tujuan pengamanan. Biasanya digunakan secara bersama-sama dengan kartu magnetis ataupun sarana lainnya.
Predictive Maintenance	Suatu bentuk pemeliharaan untuk mengetahui kesalahan jauh hari sebelum terjadi.
Preventive Maintenance	Suatu bentuk pemeliharaan untuk menjaga sebelum kesalahan terjadi.
Public Shared routed	Suatu jaringan antara yang digunakan untuk akses oleh *network* publik maupun bersama.
Saluran Transmisi	Sarana komunikasi untuk mengirimkan data dari suatu lokasi ke satu atau lebih lokasi penerima, baik melalui saluran telepon umun, khusus, satelit, ataupun saluran komunikasi lainnya.
Security log	Catatan-catatan yang berkaitan dengan keamanan hardware/software.
Security System	Sistem yang digunakan untuk pengamanan fisik dan pengamanan logik terhadap teknologi infromasi.
Shareware	Adalah perangkat lunak umum yang didistribusikan terlebih dahulu oleh penciptanya dengan pemahaman bahwa pemakai akan membayarnya kemudian setelah pemakaian memutuskan untuk tetap menggunakannya.
Sistem terbuka	Suatu kerangka sistem yang dapat diakses oleh pihak lain.

Sistem Utama	Adalah sistem yang mencatat kegiatan operasional BPKP, dan aset-aset utama BPKP, seperti sistem informasi Hasil Pengawasan, sistem informasi Kepegawaian, sistem informasi Keuangan dan Perlengkapan, dan sistem-sistem lainnya yang telah disetujui oleh Kepala BPKP atau Kepala Pusinfowas untuk mendapat prioritas pemulihan pada kondisi darurat.
Staging Area	Adalah suatu tempat (lokasi, letak domain, media penyimpan) yang terpisah dari sistem produksi dan dirancang untuk area uji coba sistem sebelum sistem tersebut dioperasikan di area produksi.
System Backup and Recovery	Merupakan salah satu area dalam *disaster* dan *recovery plan,* mencakup penyiapan *backup* perangkat keras/lunak dari sistem yang dioperasikan, beserta sistem dan prosedur yang dibuat untuk mengatasi segala permasalahan/bencana yang mungkin timbul.
System Log	Catatan-catatan yang berkaitan dengan akses ke suatu sistem.
Transport Control protocol (TPC)/Internet Protocol (IP)	Sebuah kumpulan lebih dari seratus *Protocol* dan *tool* yang membentuk fundamen internet dan Intranet. *TCP/IP* diadopsi sebagai standar jaringan.
ValidasiData	Menguji dan mencetak kebenaran dari suatu data transaksi.
Virus	Adalah program komputer yang mampu memperbanyak diri dengan cara menyertakan kode program virus tersebut ke dalam file atau program lainnya. Secara umum, virus dapat merusak/menganggu data atau file dalam PC.
Voice Mail	Fasilitas pada sistem PBX yang digunakan untuk merekam pesan yang diterima oleh extension telepon tertentu.
Wide Area Network (WAN)	Jaringan komputer dan beberapa komputer atau LAN yang saling berhubungan satu sama lain, dimana jaringan komputer tersebut berada di berbagai tempat/gedung/lokasi. Misal, jaringan komputer di BPKP Pusat dengan jaringan komputer di BPKP Perwakilan di semua Provinsi.

II. PENDAHULUAN

BPKP mengemban sebagian tugas dan misi pemerintah di bidang pengawasan yang cukup berat sekaligus strategis. Sebagai upaya untuk menunjang kelancaran dan kegiatan operasional di bidang tersebut, maka BPKP memerlukan sistem dan teknologi informasi informasi yang memadai, baik perangkat keras ataupun perangkat lunak, dan sumber daya manusianya.

Implementasi sistem dan teknologi informasi yang digunakan di lingkungan BPKP harus dilakukan dengan mempertimbangkan aspek manfaat, efisiensi, dan keamanaf agar tujuan penerapan sistem dan teknologi informasi (selanjutnya disebut teknologi informasi) dapat tercapai secara optimal.

Dalam pelaksanaannya, seluruh lingkup kegiatan bidang teknologi informasi tersebut di atas dikoordinasikan oleh Pusat Informasi Pengawasan (selanjutnya disingkat Pusinfowas) BPKP.

A. Tugas dan Fungsi

Sesuai pasal 257 Surat Keputusan Kepala BPKP Nomor: Kep-06.00.00-080/K/ 2001 tanggal 20 Pebruari 2001, menyebutkan bahwa Pusinfowas mempunyai

tugas: “melaksanakan pengelolaan data dan informasi serta pengembangan sistem informasi”.

Selanjutnya pada pasal 258 dinyatakan bahwa dalam melaksanakan tugas sebagaimana dimaksud dalam pasal 257 tersebut, Pusinfowas menyelenggarakan fungsi :

a. Penyusunan rencana dan program pengelolaan data dan informasi serta pengembangan sistem informasi;
b. Pengumpulan, pengolahan, dan penyajian data dan informasi serta administrasi basis data;
c. Penyiapan kompilasi analisis hasil pengawasan;
d. Pengembangan sistem informasi dan pembinaan terhadap pengguna; dan
e. Pelaksanaan urusan tata usaha.

Untuk menyelaraskan substansi tugas dan fungsi tersebut, Pusinfowas memiliki beberapa konsentrasi kegiatan, yaitu sebagai berikut :

1. Mengkoordinasikan dan melaksanakan penyusunan sasaran, rencana kerja, dan anggaran tahunan teknologi informasi berdasarkan rencana pengembangan sistem informasi, infrastruktur perkantoran, sarana dan prosedur yang telah disusun.
2. Menyusun, mengembangkan, dan memantau efektivitas sistem pengendalian yang menjamin kelancaran operasional dan tersedianya infrastruktur perkantoran, sistem komputer beserta kelengkapannya, meliputi prosedur operasional rutin sistem komputer, jaringan, sistem *backup,* printer, perlengkapan *data center,* dan sebagainya, sehingga dapat senantiasa mendukung kegiatan operasiona1 BPKP.
3. Menyusun, mengembangkan, dan memantau implementasi sistem keamanan atas sistem, data, dan jaringan komputer BPKP.
4. Mengkoordinasikan dan memantau penyusunan strategi untuk menjamin kua1itas sistem yang dikembangkan, baik yang dibuat oleh staf/pegawai Pusinfowas (*inhouse*) maupun yang dibuat oleh mitra kerja (*outsource*), termasuk melakukan pengujian terhadap sistem sebelum sistem tersebut dipergunakan oleh pengguna akhir (*end-user*).
5. Mengkoordinasikan dan melaksanakan penyusunan strategi dan program pelatihan untuk membantu penguna akhir dalam menggunakan atau memanfaatkan sistem aplikasi perkantoran maupun sistem pendukung operasional perusahaan secara optimal.
6. Mengikuti perkembangan teknologi informasi, serta mengevaluasi kemungkinan diterapkannya teknologi tersebut di BPKP dengan mempertimbangkan aspek efektivitas, biaya, dan waktu penerapan.

B. Maksud Kebijakan

Kebijakan sistem dan teknologi informasi disusun dengan tujuan membentuk kesamaan sudut pandang (persepsi) dalam pengimplemtasian sistem dan teknologi informasi di lingkungan BPKP. Kebijakan bertujuan untuk melindungi kepentingan BPKP atas risiko yang mungkin akibat penyalahgunaan fasilitas teknologi informasi di lingkungan BPKP, serta meningkatkan efisiensi dan efektivitas pemanfaatan teknologi informasi lingkungan BPKP.

Kebijakan sistem dan teknologi informasi ini mencakup kebijakan yang terkait dengan: penggunaan sistem e-mail dan internet; keamanan asset teknologi informasi; pengembangan perangkat lunak; pengelolaan pusat data; pengelolaan jaringan dan akses ke jaringan komputer baik di tingkat *local area network* (LAN), *metropolitan area network* (MAN), maupun *wide area network* (WAN) investasi perangkat keras dan perangkat Lunak; dan penanganan/penanggulangan bencana *(disaster recovery plan).*

Kebijakan ini diharapkan dapat menjadi landasan kegiatan operasional pengelolaan perangkat keras dan perangkat lunak teknologi informasi di lingkungan BPKP.

Untuk peningkatan kinerja BPKP, Pusinfowas diposisikan sebagai pelayanan sistem dan teknologi informasi, baik bagi user di lingkungan BPKP *(internal user)* maupun *user* dari luar BPKP *(extemal user).*

C. Sistematika Kebijakan

Sistematika kebijakan yang akan diuraikan berikut ini terdiri dari:

- PENDAHULUAN
- SISTEM E-MAIL VIA INTRANET DAN INTERNET
- PENGELOLAAN DATA DAN PERANGKAT LUNAK
- KEAMANAN ASET TEKNOLOGI INFORMASI
- PENGENDALIAN AKSES KE DALAM SISTEM BPKP
- JARINGAN KOMPUTER BPKP
- PENGEMBANGANPERANGKATLUNAK
- *DISASTER RECOVERY PLAN*
- KEBIJAKAN LAIN-LAIN.

D. Penerapan Teknologi

Penggunaan teknologi informasi di lingkungan BPKP dimaksudkan untuk mendukung kegiatan operasional BPKP dalam mencapai target dan rencan kerja BPKP secara akurat, tepat waktu, dan terkendali.

Teknologi informasi yang diterapkan di lingkungan BPKP wajib mempertimbangkan aspek tepat guna, tepat waktu, efisiensi, keterpaduan da memperhatikan arah perkembangan teknologi informasi secara umum, seperti penggunaan *open system* dan *open architecture,* dengan tetap mengutamakan kesesuaian alur kerja dan prosedur operasional BPKP.

E. Investasi Perangkat Teknologi Informasi

Semua investasi perangkat teknologi informasi harus dikoordinasikan dengan Pusinfowas untuk memastikan tidak terjadi duplikasi dan menjaga integrasi serta kompatibilitasnya terhadap perangkat keras maupun perangkat lunak yang telah ada.

Pusinfowas senantiasa melakukan studi kelayakan untuk mengoptimalkan penggunaan perangkat teknologi yang telah ada dan dapat merekomendasikan investasi perangkat teknologi yang tepat untuk mendukung operasional kerja BPKP.

F. Pengendalian Mutu

Setiap implementasi teknologj informasi di lingkungan BPKP harus melalui tahapan pengendalian mutu yang ditetapkan. Pelaksanaan pengendalian mutu dilakukan dengan menggunakan beberapa parameter, seperti tingkat konsistensi, tingkat pemenuhan jadwal kerja, dan standar-standar unjuk kerja. Semua parameter tersebut harus didokumentasikan dengan baik.

G. Pemeliharaan

Semua perangkat teknologi informasi yang telah dimiliki BPKP harus dapat dioptimalkan melalui :

- Pemeliharaan secara rutin yang dilakukan terhadap semua perangkat teknologi yang ada meliputi pemeliharaan perangkat keras baik yang terintegrasi dalam jaringan maupun perangkat keras yang berdiri sendiri; perangkat lunak; dan database sehingga dapat meminimalkan resiko kerusakan sistem.
- Tersedianya *back up* baik software maupun data dalam sistem *library* yang memadai.
- Penambahan fitur dan fasilitas yang dapat dikembangkan dari sistem yang telah ada.
- Pemanfaatan kapasitas sistem secara maksimal sebelum diputuskan untuk pembelian/investasi sistem baru.

- Pemeliharaan dari pengembangan *software* yang berasal dari *in house* ataupun *out sourcing* dalam satu koordinasi dengan pemeliharaan rutin.
  Pusinfowas akan secara proaktif mengingatkan pengguna sistem agar dapat mengoptimalkan sumber daya sistem yang telah ada.

H. Keamanan Sistem
Keamanan system, data dan informasi bagi BPKP merupakan hal yang utama, sehingga setiap sistem harus dilengkapi dengan keamanan sistem yang baik dan diawasi secara berkesinambungan untuk memproteksi data dan informasi dari akses para pihak yang tidak berwenang. Untuk mencapai hal tersebut, perlu dilakukan studi kelayakan dan studi perbandingan produk keamanan sistem yang paling sesuai bagi kebutuhan BPKP.

I. Sumber Daya Manusia
Dalam upaya menjaga kelancaran operasional teknologi informasi, maka BPKP memerlukan sumber daya manusia yang memiliki kemampuan untuk mengelola teknologi informasi yang diterapkan melalui pelatihan dan pembekalan yang memadai.

III. SISTEM E-MAIL VIA INTRANET DAN INTERNET

Kebijakan yang tercakup dalam bagian ini terdiri dari :
Kebijakan 1 : Kepemilikan sistem e-mail
Kebijakan 2 : Pengguna sistem e-mail
Kebijakan 3 : Pemanfaatan sistem e-mail
Kebijakan 4 : Isi E-mail
Kebijakan 5 : Keamanan sistem e-mail
Kebijakan 6 : Penggunaan Intranet
Kebijakan 7 : Penggunaan Internet
Lingkup Kebijakan :

- Kebijakan ini diberlakukan untuk seluruh pimpinan, pegawai, dan mitra kerja BPKP.
- Kebijakan ini meliputi semua aspek yang terkait dengan penggunaan e-mail dan Internet.
- Pelanggaran atas kebijakan ini dapat mengakibatkan diberikannya sanksi-sanksi disipliner sesuai ketentuan yang berlaku di BPKP.

A. Kepemilikan sistem e-mail
1. Sistem e-mail yang digunakan di lingkungan BPKP dimiliki oleh BPKP dan dikelola secara penuh oleh Pusinfowas.
2. Sistem e-mail BPKP hanya dipergunakan untuk kepentingan BPKP, dan tidak diperkenankan untuk kepentingan pribadi. Seluruh e-mail yang dibuat, dikirimkan, dan diterima melalui jaringan komputer dan atau sistem e-mail BPKP menjadi milik BPKP.
3. BPKP berhak untuk :

a. Melakukan pengawasan dan pemeriksaan atas e-mail yang dibuat, dikirim, dan diterima melalui jaringan komputer dan atau melalui sistem e-mail, termasuk melakukan pemeriksaan atas isi e-mail jika diperlukan
b. Melakukan perubahan atas pembatasan volume/ukuran e-mail, waktu pemakaian, dan hal-hal lain demi kepentingan BPKP dengan memperhatikan ketersediaan sumber daya sistem yang ada.
c. Melakukan pembekuan, penghapusan, pembatalan pengiriman dan penerimaan e-mail, atau proses lain yang terkait dengan sistem e-mal jika dipandang perlu, demi kepentingan dan keamanan BPKP.

4. BPKP akan menjamin hal-hal yang bersifat pribadi dari pengguna sistm e-mail.

5. Seluruh pesan e-mail walaupun telah dihapus oleh pengguna, diupayakan masih tercatat dan tersimpan dalam server *(e-mail server)* dan atau media penyimpanan *backup.*
6. Backup atas data e-mail hanya dapat *di-restore* dan digunakan untuk keperluan pemulihan pada kondisi *disaster* dan atau untuk kepentingan BPKP.
7. Pusinfowas benanggungjawab untuk melakukan perawatan, pengoperasian, perubahan konfigurasi dan pelaporan sistem e-mail, termasuk hal-hal yang dianggap perlu.

B. Pengguna sistem e-mail
   1. Pengguna sistem e-mail adalah seluruh pimpinan, pegawai, dan mitra kerja BPKP, serta pihak lain yang telah mendapat persetujuan secara tertulis dari Kepala Pusinfowas.
   2. Pengguna sistem e-mail bertanggungjawab atas kegiatan pengelolaan dan *mailbox* masing-masing, termasuk menghapus pesan-pesan yang sudah tidak diperlukan.
   3. Pengguna sistem e-mail bertanggung jawab atas isi pesan yang dibuatnya termasuk jika terjadi tindakan hukum yang dikenakan atas isi pesan tersebut. BPKP tidak dapat dikenakan pertanggungjawaban secara hukum berkenaan dengan isi pesan yang dibuat oleh pengguna sistem e-mail.
   4. Pengguna sistem e-mail dapat memanfaatkan fasilitas ini untuk keperluan pekerjaan dan sepanjang jam kerja yang telah ditetapkan BPKP. Dalam hal diperlukan akses terhadap sistem e-mail dari luar kantor, maka pengguna harus mengajukan permohonan kepada Pusinfowas.
   5. Pengguna sistem e-mail hanya dapat melakukan akses ke sistem e-mail BPKP dengan menggunakan perangkat lunak yang ditentukan oleh Pusinfowas.
   6. Pengguna sistem e-mail akan memperoleh *mailbox* dalam *server dengan* kapasitas sebagaimana ditetapkan oleh Pusinfowas.

C. Pemanfaatan sistem e-mail
   1. Data dan informasi yang bersifat Sangat Rahasia, Rahasia dan Konfidensial tidak diperkenankan dikirim menggunakan sistem e-mail kecuali :
      a. Disetujui terlebih dahulu oleh pimpinan pemilik data dan informasi *(data owner)*
      b. Dikirimkan dalam bentuk. yang teracak *(encrypted)* dan disertai dengan peringatan bahwa isi pesan yang dikirim bersifat Sangat Rahasia, Rahasia. dan Konfidensial, dan informasi tersebut adalah milik BPKP.
   2. Sistem e-mail tidak diperkenankan digunakan untuk hal-hal sebagai berikut:
      a. Pembuatan dan penyebaran surat berantai *(chain letters).*
      b. Pembahasan hal-hal yang berkaitan dengan kegiatan politik.
      c. Penyampaian pesan yang isinya bertentangan dengan hukum, aturan, dan kode etik, termasuk pelecehan dan ancaman.
      d. Penyampaian pesan yang berasal dari sumber yang tidak dapat dipertanggung jawabkan kebenarannya, seperti surat kaleng, rumor, dan sejenisnya.
      e. Pengiriman pesan untuk keuntungan pribadi.
      f. Pengambilan dan pengiriman pesan dalam bentuk file yang tidak berkaitan dengan kegiatan kantor BPKP.
      g. Penyebaran informasi kepada seluruh pengguna sistem e-mail untuk hal-hal yang tidak berkaitan dengan kegiatan kantor BPKP.
   3. Pengguna sistem e-mail harus berhati-hati dalam membuka *attachment* yang ada dalam suatu e-mail. Dalam hal diterima *attachment* yang tidak jelas dan tidak berkaitan dengan kegiatan kantor BPKP, atau diterima dari pengirim yang tldak dikenal, maka e-mail tersebut harus disampalkan kepada Pusinfowas untuk diperiksa.
   4. Alamat e-mail BPKP (*e-mail address)* tidak diperkenankan digunakan untuk hal-hal yang tidak berkaitan langsung dengan tugas dan pekerjaan di BPKP;

5. Pesan yang akan disebarkan ke seluruh pengguna sistem e-mail harus mendapatkan persetujuan dari kepala satuan kerja yang bersangkutan.

D. Isi E-mail
   1. Pengguna sistem e-mail bertanggung jawab atas isi dan pesan yan disampaikan.
   2. Semua pengiriman e-mail ke luar lingkup BPKP harus mencantumkan pernyataan *disclaimer* sekurang-kurangnya sebagai berikut :
      The information contained in this communication is ittended solely for use of the individual or entity to whom it is addressed and others authorized to receive it. It may contain confidential or legally previliged information. Unless otherwise specifically stated by sender, any documents or views presented are solely those of the sender and do not constitute official documents and views of BPKP (Badan Pengawasan Keuangan dan Pembangunan/FDSB = The Financial and Development Supervisory Board).
   3. Isi e-mail yang dikirimkan tidak diperbolehkan berisi hal-hal yang bertentangan dengan norma umum dan kode etik yang berlaku.
   4. Setiap orang yang merasa tergangu dengan isi e-mail yang diterima dapat segera melaporkannya kepada Pusinfowas.
   5. Penyalahgunaan e-mail yang dilakukan akan dilaporkan kepada Pusinfowas dan instansi terkait lainnya.
   6. Ukuran isi e-mail dalam satu kali pengiriman tidak boleh melebihi ketentuan yang ditetapkan oleh Pusinfowas.

E. Keamanan Sistem e-mail
   1. Pengguna e-mail akan mendapatkan satu *account* dari Pusinfowas yang dilengkapi dengan *password.*
   2. Pengguna e-mail bertanggung jawab atas *account* dan *password* yang diberikan tersebut.
   3. Koneksi sistem e-mail dengan sistem e-mail lain di luar lingkungan BPKP harus dilengkapi dengan perangkat keamanan yang memadai dan memiliki kemampuan:
      a. Melindungi informasi struktur jaringan BPKP.
      b. Melakukan karantina terhadap e-mail yang diperkirakan akan mengganggu dan atau merusak sistem di BPKP.
      c. Menambahkan kalimat *disclaimer* pada setiap pengiriman e-mail dari BPKP.
   4. Koneksi sistem e-mail BPKP dengan sistem e-mail lain di luar lingkungan BPKP akan diatur lebih lanjut oleh Pusinfowas.

F. Penggunaan Intranet
   1. Pusinfowas bertanggung jawab untuk menyediakan fasilitas komunikasi data maupun persuratan untuk keperluan intern melalui jaringan BPKP.
   2. Informasi yang terhubung melalui internet diklasifikasikan sesuai sifatnya melalui keputusan pihak yang terkait, kemudian akses diberikan sesuai dengan kewenangan masing-masing.
   3. Informasi yang bersifat umum dapat di share kepada seluruh pegawai dikoordinasikan dengan mail administrator.
   4. User dilarang meletakkan *(posting) software* dan informasi untuk keperluan intern ke dalam media *Intranet* yang dapat diakses seluruh pegawai BPKP tanpa melalui izin atasan/pimpinan terlebih dahulu.

G. Penggunaan Internet
   1. Pusinfowas bertanggung jawab untuk mengatur hak akses ke Internet termasuk pengaturan jalur koneksi, jenis layanan (service), kecepatan, dan waktu akses.

2. Koneksi ke Internet harus dilengkapi dengan perangkat keamanan yang memadai dengan kemampuan:
   a. Melindungi informasi struktur jaringan BPKP.
   b. Menentukan jenis layanan *(services),* waktu akses, dan pengguna yang diperbolehkan untuk koneksi ke internet.
   c. Mencatat pada jejak audit *(audit trail)*.
   d. Mendeteksi dan mencatat adanya usaha-usaha pengaksesan jaringan internal oleh pihak yang tidak berhak.
   e. Melakukan pengacakan data *(data encryption)* jika diperlukan.
   f. Koneksi secara *dial up* dengan menggunakan fasilitas kantor tidak diizinkan.
3. Permintaan koneksi ke internet melalui Jaringan BPKP harus mendapatkan persetujuan dari atasan/pimpinan pengguna dan Pusinfowas.
4. Internet hanya dipergunakan untuk mendukung tugas dan kegiatan dinas BPKP.
5. Pengguna internet tidak diperkenan mengakses dan atau mengambil (*download)* file, informasi, data yang bertentangan dengan hukum, aturan dan kode etik/kesusilaan, termasuk pelecehan dan ancaman, serta kegiatan yang berkaitan dengan politik. Adanya fasilitas yang dapat digunakan untuk akses ke alamat/*site* tersebut tidak dapat diartikan bahwa user telah diberikan izin untuk akses.
6. Dalam hal terjadinya penyimpangan penggunaan koneksi internet, Pusinfowas berhak untuk mencabut hak akses pengguna ke internet.
7. Seluruh pengguna internet harus menyadari segala resiko yang timbul akibat penggunaan fasilitas internet.
8. Download data yang berasal dari luar jaringan komputer intern BPKP harus *di-scan* menggunakan software pendeteksi virus terlebih dahulu.
9. User dilarang meletakkan *(posting) software* dan informasi untuk keperluan intern ke dalam media internet yang dapat diakses publik tanpa melalui izin atasan/pimpinan terlebih dulu.

IV. PENGELOLAAN DATA DAN PERANGKAT LUNAK

Kebijakan yang tercakup dalam bagian ini terdiri dari :
Kebijakan 1 : Kepemilikan data *(Data Owner)*
Kebijakan 2 : Kustodi Data dan Sistem *(Data and System Custodian)*
Kebijakan 3 : Perangkat Lunak
Kebijakan 4 : Peningkatan Versi Perangkat Lunak
Kebijakan 5: Perangkat Lunak Umum
Kebijakan 6: Keamanan Informasi
Lingkup Kebijakan :

- Kebijakan ini diberlakukan untuk seluruh pimpinan, pegawai, dan mitra kerja BPKP.
- Kebijakan ini mencakup semua aspek mengenai kepemilikan data dan perangkat lunak, serta pengelolaannya.
- Pelanggaran atas kebijakan ini dapat mengakibatkan diberikannya sanksi-sanksi disipliner sesuai ketentuan yang berlaku di BPKP.

A. Kepemilikan Data

1. Semua data dan informasi yang dihasilkan dan atau dikumpulkan oleh pegawai maupun pejabat BPKP, baik langsung maupun melalui mitra kerja, selama bekerja untuk BPKP merupakan milik BPKP.
2. Pemilik data *(Data Owner)* adalah pegawai/pejabat pimpinan BPKP yang bertanggungjawab atas semua data dan informasi yang dihasilkan, dikelola dan atau dikumpulkannya selama bekerja untuk BPKP.
3. Data dan informasi milik BPKP tidak diperbolehkan untuk ditransfer diberikan, atau dipinjamkan kepada organisasi atau individual lain di luar

BPKP, kecuali bagi kepentingan BPKP dengan persetujuan tertulis dari pemilik data.

4. Empat jenis/kriteria data yang dikelola BPKP adalah :
   a. Sangat Rahasia (SR) : Surat (data) yang informasinya membutuhkan tingkat pengamanan yang tertinggi. Tingkat pengamanan informasi surat (data) erat hubungannya dengan keamanan dan keselamatan negara serta hanya boleh diketahui oleh pejabat yang berhak menerimanya.
   b. Rahasia (R): Surat (data) yang informasinya membutuhkan tingkat pengamanan yang tinggi. Tingkat pengamanan informasi surat (data) erat hubungannya dengan keamanan kedinasan dan hanya boleh diketahui oleh pejabat yang berwenang atau yallg ditunjuk.
   c. Terbatas/Konfidensial (K) : Surat (data) yang informasinya membutuhkan tingkat pengamanan yang tinggi. Tingkat pengamanan informasi surat (data) erat hubungannya dengan tugas khusus kedinasan dan hanya boleh diketahui oleh pejabat yang berwenang atau yang ditunjuk.
   d. Biasa: Surat (data) yang tidak memerlukan pengamanan khusus.
5. *Data Owner* bertanggung jawab untuk mengelompokkan data berdasarkan definisi jenis data tersebut diatas.
6. Persetujuan pemberian akses terhadap data dilakukan oleh *Data Owner,* dengan memperhatikan jenis/kriteria data yang telah mereka tetapkan.
7. Permasalahan yang tidak terselesaikan dalam pemberian akses terhadap data wajib disampaikan kepada Kepala BPKP untuk dapat ditindaklanjuti sesuai ketentuan yang berlaku.

B. Kustodi Data dan Sistem
   1. Tugas dan tanggung jawab Kustodi Data dan Sistem termasuk -tapi tidak terbatas pada-hal-hal di bawah ini:
      a. Melakukan proses *backup* secara berkala sesuai kesepatkatan dengan *Data Owner*.
      b. Menyimpan dan mengelola media penyimpanan hasil proses *backup* di tempat yang aman dan terpisah dari tempat originalnya.
      c. Melakukan verifikasi atas hasil *backup* secara acak minimal dua bulan sekali.
      d. Melakukan *proses restore* data sesuai permintaan dari *Data Owner* selama tidak bertentangan dengan ketentuan yang berlaku.
      e. Mengelola sistem yang digunakan.
      f. Melakukan dukungan teknis dan pemeliharaan terhadap sistem aplikasi sesuai kesempatan dengan *Data Owne7:*
   2. Proses pemeliharaan sistem aplikasi meliputi hal di bawah ini :
      a. Corrective maintenance
      b. Detective maintenance
      c. Preventive maintenance
      d. Predictive maintenance
   3. Proses restore dapat dilakukan dalam kondisi di bawah ini :
      a. Adanya permintaan dari *Data Owner* dengan persetujuan Kepala/Pejabat Pimpinan dari *Data Owner* tersebut.
      b. Terjadinya gangguan pada sistem pengolah data tersebut, dengan persetujuan Pusinfowas dan pimpinan dari *Data Owner.*
      c. Adanya permintaan dari Kepala BPKP.

C. Perangkat Lunak
   1. Semua perangkat lunak, baik yang dibuat atau dibeli oleh BPKP, merupakan milik BPKP dan tidak dapat ditransfer, diedarkan atau dipinjamkan kepada pihak lain di luar BPKP tanpa persetujuan Pusinfowas.
   2. Pengadaan perangkat lunak di lingkungan BPKP harus dikoordinasikan dengan Pusinfowas.

3. Semua perangkat lunak yang menjadi milik BPKP dipasang *(install)* oleh petugas yang ditunjuk oleh Kepala Pusinfowas.
4. Permintaan instalasi perangkat lunak khusus dalam rangka pemenuhan tugas dan tanggung jawab BPKP, dilakukan dengan persetujuan Kepala/Pejabat Pimpinan terkait dan Kepala Pusinfowas.
5. Setiap pengguna perangkat lunak milik BPKP wajib membaca dan memahami ketentuan tentang lisensi perangkat lunak tersebut.
6. Perangkat lunak yang dipasang di BPKP harus memiliki lisensi atau seizin tertulis pemiliknya.
7. Semua perangkat lunak milik BPKP termasuk bukti lisensi perangkat lunak tersebut disimpan dan diadministrasikan secara terpusat di Pusinfowas.

D. Peningkatan Versi Perangkat Lunak
1. Setiap rencana peningkatan versi perangkat lunak dari versi yang lama ke versi yang lebih baru wajib dikaji terlebih dahulu oleh Kustodi Data dan Sistem sebelum peningkatan versi perangkat lunak diberlakukan di lingkungan BPKP.
2. Kustodi Data dan Sistem bertanggungjawab memantau dan mengkaji semua perubahan perangkat lunak, *pathces, bugs,* dan versi baru serta membuat ketentuan yang buhubungan dengan waktu dan tata cara penerapan versi perangkat lunak yang baru dilingkungan BPKP.

E. Perangkat Lunak Umum
1. Penggunaan s*hareware* dan *freeware* harus dikaji terlebih dahulu dan disetujui oleh Pusinfowas sebelum dapat digunakan di lingkungan produksi.
2. Penggunaan perangkat lunak versi demo dapat dilakukan untuk mendukung proses pengujian perangkat lunak sebelum dilakukan pembelian perangkat lunak tersebut.
3. Setiap pemakai perangkat lunak umum *(shareware, freeware*/*demo)* wajib memahami *resiko* digunakannya perangkat lunak tersebut.

F. Keamanan Informasi
Semua informasi/data dalam bentuk elektomik yang bersifat Sangat Rahasia, Rahasia, Konfidensial, Biasa dan sudah tidak dipergunakan di lingkungan BPKP harus dikelola sesuai dengan ketentuan tentang pemusnahan/pemisahan dokumen atau jadwal retensi arsip.

V. KEAMANAN ASET TEKNOLOGI INFORMASI

Kebijakan yang tercakup dalam bagian ini terdiri dari :
Kebijakan 1 : Keamanan Fisik
Kebijakan 2 : Pengelolaan Keamanan Sistem
Kebijakan 3 : Pengujian Keamanan
Kebijakan 4 : Penanggulangan Virus
Kebijakan 5 : Manajemen Konfigurasi Sistem
Kebijakan 6 : Pemeliharaan Sistem
Lingkup Kebijakan :
- Kebijakan ini diberlakukan untuk seluruh pimpinan, pegawai, dan mitra kerja BPKP.
- Kebijakan ini meliputi semua aspek keamanan dan aset-aset teknologi informasi yang dimiliki BPKP.
- Pelanggaran atas kebijakan ini dapat mengakibatkan diberikannya sanksi-sanksi disipliner sesuai ketentuan yang berlaku di BPKP.

A. Keamanan Fisik
1. Server-server operasional yang digunakan untuk menyimpan dan mengolah data informasi BPKP harus ditempatkan di ruang Pusat Data yang ditetapkan oleh Pusinfowas.

2. Pusat Data harus dilengkapi perangkat-perangkat yang menjamin agar lingkungan Pusat Data memenuhi standar untuk beroperasinya server-server, termasuk, tetapi tidak terbatas, pendingin udara *(Air Condition), Uninterupted Power Supply (UPS),* dan sistem pemadam kebakaran.
3. Pusat Data harus dilengkapi dengan perangkat keamanan sehingga hanya petugas berwenang yang dapat memasuki ruangan Pusat Data.
4. Pusat Data harus dilengkapi dengan mekanisme untuk memonitor keadaan pada ruangan tersebut.
5. Perubahan konfigurasi maupun pengelolaan server-server BPKP hanya dapat dilakukan melalui monitor *(console)* yang ditempatkan di ruangan yang aman.
6. Perubahan konfigurasi secara tidak langsung/jarak jauh *(remote)* hanya dapat dilakukan setelah mendapat persetujuan dari Pusinfowas.
7. Akses ke ruangan Pusat Data hanya dapat dilakukan oleh petugas berwenang yang ditunjukan oleh Pusinfowas. Pihak lain yang melakukan kegiatan sehubungan dengan tugasnya di Pusat Data harus mendapatkan persetuJuan (izin) dari Pusinfowas dan diawasi oleh petugas berwenang.

B. Pengelolaan Keamanan Sistem
1. Setiap pengguna system komputer BPKP bertanggungjawab atas aktivitasnya masig-masing.
2. Setiap aktivitas pengguna harus dicatat dalam bentuk jejak audit sistem.
3. Segala bentuk akses logik *(Logical access)* ke Pusat Data (*Data Center*) tidak diperkenankan, kecuali diizinkan secara khusus oleh pusinfowas sesuai dengan ketentuan yang berlaku.
4. Pengelola Pusat Data BPKP wajib menggunakan identifikasi khusus *(user id)* yang diberikan, dan tidak diperkenankan untuk menggunakan *user id* secara bersama *(share)*.
5. Untuk memudahkan pengelolaan dan memonitor keamanan maka beberapa server yang memiliki konfigurasi keamanan yang serupa dikelompokkan dalam satu domain.
6. Komunikasi antar domain harus mendapat persetujuan terlebih dahulu dari Pusinfowas dengan memperhatikan keamanan masing-masing domain.
7. Akses pengelola Pusat Data ke dalam setiap sistem komputer harus tercatat dalam jejak audit sistem yang meliputi waktu akses dan aktivitas yang dilakukan selama akses ke dalam sistem.
8. Kepala pusinfowas secara berkala atau apabila diminta oleh Kepala BPKP berhak dan wajib untuk memeriksa jejak audit sistem, termasuk namun tidak terbatas pada *security log, system log, application log,* dan melaporkan penyimpangan yang ditemukan kepada Kepala BPKP atau Pejabat lain yang ditunjuk.
9. Perubahan konfigurasi atau penyampaian perintah operasi dari jarak jauh melalui jaringan komputer hanya dapat dilakukan dengan mekanisme otentikasi yang ditetapkan oleh Pusinfowas.

C. Pengujian Keamanan
1. Sistem keamanan perangkat keras dan perangkat lunak yang akan digunakan di jalur publik harus diuji sebelum dioperasikan, dan diuji ulang sekurang-kurangnya sekali dalam satu tahun.
2. Jadwal dan ruang lingkup pengujian keamanan harus mendapat persetujuan dari Pusinfowas.
3. Pengujian keamanan dilakukan oleh pejabat yang ditunjuk oleh Kepala Pusinfowas.
4. Hasi1 pengujian harus dilaporkan kepada Kepala Pusinfowas untuk ditindaklanjuti.

D. Penanggulangan Virus

1. Pusinfowas menyiapkan prosedur standar penanggulangan virus dan disosialisasikan ke seluruh pengguna sistem komputer.
2. Setiap pengguna sistem komputer BPKP wajib menjalankan prosedur penanggulangan virus secara benar dan konsisten.
3. Setiap data dan program komputer yang ditransmisikan secara elektronis ke dalam sistem komputer BPKP harus diperiksa untuk mendeteksi keberadaan virus sebelum digunakan.
4. Semua data dan program komputer di lingkungan sistem komputer BPKP harus diperiksa untuk mendeteksi keberadaan virus secara berkala.
5. Semua PC dan *server* di lingkungan sistem komputer BPKP harus dilengkapi dengan perangkat lunak pendeteksi virus yang disetujui oleh Pusinfowas.
6. Perangkat lunak pendeteksi virus harus selalu aktif selama komputer tersebut dioperasikan.
7. Pusinfowas memastikan bahwa perangkat lunak pendeteksi virus diperbaharui secara berkala.
8. Seluruh pengguna sistem BPKP dilarang membuat atau menyebarkan atau menggunakan perangkat lunak yang diketahui atau diduga mengandung virus ke dalam sistem komputer BPKP.
9. Setiap virus yang ditemukan di lingkungan BPKP harus dilaporkan kepada Pusinfowas untuk diteliti dan ditanggulangi penyebarannya.

E. Manajemen Konfigurasi Sistem

1. Setiap perubahan konfigurasi di lingkungan produksi harus mendapat persetujuan dari Kepala/Pimpinan unit yang bersangkutan dan Kepala Bidang Pengembangan Sistem Informasi.
2. Setiap perubahan konfigurasi di lingkungan produksi harus terlebih dahulu dievaluasi dan diujicobakan di lingkungan pengembangan *(staging area).*
3. Pusinfowas melakukan evaluasi atas perubahan konfigurasi yang dilakukan di lingkungan produksi.
4. Setiap perubahan konfigurasi di lingkungan produksi harus dicatat secara terpusat. Catatan perubahan konfigurasi dapat berbentukjejak audit sistem.
5. Pusinfowas harus melakukan pengkajian terhadap konfigurasi sistem di lingkungan produksi secara berkala untuk mendukung kinerja sistem.

F. Pemeliharaan Sistem

1. Perangkat keras dan perangkat lunak pada Pusat Data harus diperiksa dan dipelihara secara berkala oleh pejabat yang ditunjuk oleh Kepala Pusinfowas.
2. Perangkat keras dan perangkat lunak pada Pusat Data yang digunakan untuk operasional sistem utama BPKP wajib dipelihara secara khusus sehingga tingkat ketersediaan dan unjuk kerja sistem tersebut memenuhi standar yang disepakati.
3. Pemeliharaan perangkat kerja dan perangkat lunak dapat dilakukan melalui perjanjian kerja dengan mitra kerja yang memiliki kompetensi di bidangnya.
4. Perjanjian pemeliharaan perangkat keras dan perangkat lunak dengan mitra kerja sekurangnya mencakup :
   a. Lingkup pemeliharaan;
   b. Waktu yang diperlukan untuk menanggapi masalah *(Response time);*
   c. Kunjungan berkala (khusus perangkat keras);
   d. Pemberian *patches, bugs fixes,* perubahan versi (khusus perangkat lunak).

VI. PENGENDALIAN AKSES KE DALAM SISTEM BPKP

Kebijakan yang tercakup dalam bagian ini terdiri dari :

Kebijakan 1 : Pengamanan Hak Akses Pengguna

Kebijakan 2 : Otentikasi dan Pencatatan Akses

Kebijakan 3 : Akses oleh Mitra Kerja

Kebijakan 4 : Akses dari luar BPKP
Lingkup Kebijakan :

- Kebijakan ini diberlakukan untuk seluruh pimpinan, pegawai, dan mitra kerja BPKP.
- Kebijakan ini mencakup semua aspek mengenai pengaturan dan pengendalian akses ke sistem BPKP.
- Pelanggaran atas kebijakan irii dapat mengakibatkan diberikannya sanksi-sanksi disipliner sesuai ketentuan yang berlaku di BPKP.

A. Pengamanan Hak Akses Pengguna
   1. Seluruh pejabat (pimpinan) dan pegawai BPKP diberi hak untuk mengakses sistem BPKP atas persetujuan *Data Owner* sesuai dengan ketentuan yang berlaku.
   2. Gangguan dalam mengakses sistem BPKP harus segera dilaporkan ke Pusinfowas untuk ditindaklanjuti.
   3. Setiap pengguna sistem BPKP wajib melaporkan indikasi atas penyalahgunaan hak akses kepada Pusinfowas.
   4. Untuk menjaga kerahasiaan informasi, *Data Owner* baik langsung maupun melalui Kustodi Data dan Sistem menentukan hak akses atas informasi yang disimpan pada sistem BPKP.
   5. Hak untuk mengakses sistem dan data dapat dikelompokkan dalam beberapa tingkatan, yaitu hak untuk membaca, hak untuk mengubah, hak untuk menghapus, dan hak untuk memperbaiki. Tingkatan hak akses ini ditentukan oleh *DataOwner* dan didefinisikan secara lebih rinci sesuai fungsi dan tanggung jawab pengguna sistem.
   6. Akses ke sistem BPKP hanya dipergunakan untuk menjalankan tugas kedinasan BPKP.
   7. Pengelola sistem tidak bertanggungjawab atas penyalahgunaan hak akses.
   8. Dalam hal terjadinya indikasi penyimpangan penggunaan hak akses pengelola sistem wajib memberikan laporan kepada atasan/pimpinan dan *Data Owner* dan dapat ditindak lanjuti dalam bentuk pemblokiran atau penutupan hak akses.

B. Otentikasi dan Pencatatan Akses
   1. *User-ID* dan *Password* diberikan kepada pengguna sistem BPKP sebagai identitas unik dari pengguna sistem BPKP.
   2. Setiap pengguna sistem BPKP bertanggungjawab atas segala aktivitas yang dilakukan dengan menggunakan *User-ID* yang dimiliki.
   3. Pengguna sistem BPKP tidak diperkenankan memberikan *User-ID dan password* kepada orang lain dalam kondisi apapun.
   4. Seluruh pimpinan, pegawai, dan mitra kerja BPKP tidak diperkenankan untuk melakukan akses sistem BPKP menggunakan *User-ID* dan *password* yang bukan menjadi tanggung-jawabnya (bukan miliknya).
   5. Ketentuan mengenai jumlah karakter password dan frekuensi perubahan *password* ditentukan oleh Pusinfowas.
   6. Seluruh akses ke sistem BPKP oleh pengguna sistem dicatat dalam jejak audit sistem yang akan dikaji secara berkala oleh pengelola sistem.
   7. Pengguna tidak diperkenankan menggunakan *User-ID*-nya untuk masuk ke dalam jaringan *(login)* ke lebih dari satu terminal pada saat bersamaan.

C. Akses oleh Mitra Kerja
   1. *Data Owner* baik langsung maupun melalui Kustodi Data dan Sistem dapat memberikan hak akses kepada mitra kerja untuk keperluan penyelesaian penyelesaian pekerjaan BPKP.
   2. Akses oleh mitra kerja hanya dapat dilakukan melalui perangkat komputer _di lingkungan kerja BPKP.

3. Akses oleh mitra kerja yang dilakukan dari luar lingkungan BPKP harus mendapat persetujuan dari Kepala Pusinfowas dengan menggunakan mekanisme yang telah ditetapkan.

D. Akses dari Luar BPKP
   1. Akses ke sistem BPKP dari luar lingkungan BPKP hanya dapat dilakukan dengan mekanisme yang ditetapkan oleh Kepala Pusinfowas.
   2. Semua akses ke jaringan lokal BPKP dari luar lingkungan kerja BPKP harus melewati perangkat keamanan yang telah disediakan dan dikelola oleh Pusinfowas.
   3. Pengelola sistem secara rutin memeriksa jejak audit sistem untuk melihat akses yang dilakukan dari luar lingkungan BPKP. Penyimpangan akses yang ditemukan pada jejak audit sistem dilaporkan kepada Pusinfowas untuk ditindaklanjuti.

VII. JARINGAN KOMPUTER BPKP

Kebijakan yang tercakup dalam bagian ini terdiri dari :
Kebijakan 1 : Konfigurasi Jaringan Komputer
Kebijakan 2 : Pengoperasian dan Pengelolaan Jaringan Komputer
Kebijakan 3 : Otentikasi Jaringan Komputer
Kebijakan 4 : Pengendalian Akses Jaringan Komputer
Kebijakan 5 : Hubungan dengan Jaringan Eksternal
Lingkup Kebijakan :

- Kebijakan ini diberlakukan untuk seluruh pimpinan, pegawai, dan mitra kerja BPKP.
- Kebijakan ini meliputi semua aspek keamanan jaringan komputer yang dimiliki BPKP.
- Pelanggaran atas kebijakan ini dapat mengakibatkan diberikannya sanksi - sanksi disipliner sesuai ketentuan yang berlaku di BPKP.

A. Konfigurasi Jaringan Komputer
   1. Petugas yang berwenang untuk melakukan pengelolaan atas konfigurasi jaringan komputer adalah pengelola jaringan. Pengelola jaringan komputer ditetapkan oleh Pusinfowas.
   2. Konfigurasi jaringan komputer BPKP ditetapkan oleh Pusinfowas dengan mempertimbangkan aspek keamanan, kompatibilitas, kemudahan pengelolaan, dan kinerja jaringan.
   3. Perubahan konfigurasi pada jaringan komputer BPKP tidak boleh mengganggu keterpaduan jaringan komputer BPKP.
   4. Perubahan konfigurasi jaringan BPKP harus mendapat persetujuan dari Pusinfowas.
   5. Pengelolaan jaringan komputer dapat dikelompokkan dalam beberapa bagian yang terpisah untuk meningkatkan keamanan jaringan komputer dan atau untuk kerja.
   6. Pusinfowas berhak untuk menetapkan jenis layanan yang dapat digunakan pada jaringan komputer. Penggunaan jenis layanan di luar yang ditetapkan oleh Pusinfowas harus segera ditangani oleh pengelola jaringan dan dilaporkan kepada kepala Pusinfowas untuk ditindaklanjuti.
   7. Pengelolaan jaringan komputer harus dilengkapi dengan perangkat yang dapat mendeteksi dan membatasi jenis layanan pada jaringan komputer.
   8. Konfigurasi jaringan harus didokumentasikan dengan baik dan benar oleh pengelola jaringan komputer.
   9. Secara berkala Pusinfowas wajib mengkaji konfigurasi jaringan, standar dan prosedur keamanan jaringan, sekurang-kurangnya satu kali dalam satu tahun.

B. Pengoperasian dan Pengelolaan Jaringan Komputer
   1. Pengelola jaringan wajib menggunakan identitas *(user-ID)* masing-masing dalam melakukan aktivitas pengelolaan jaringan komputer.
   2. Pengelola jaringan komputer wajib memiliki catatan atas segala kegiatan yang dilakukan sehubungan dengan pengoperasian jaringan komputer, yang meliputi waktu akses dan catatan singkat mengenai aktivitas akses.
   3. Perangkat bantu jaringan hanya boleh digunakan oleh pengelola jaringan. Penggunaan perangkat bantu jaringan dimonitor secara ketat dan disimpan pada tempat yang aman bila sedang tidak digunakan.
   4. Semua perangkat pengendali jaringan komputer tersimpan dalam lokasi yang aman dan hanya dapat diakses oleh pengelolajaringan.
   5. Mekanisme pengelolaan jaringan komputer yang dilakukan dari jarak jauh harus mendapat persetujuan dari Pusinfowas.

C. Otentikasi Jaringan Komputer
   1. Semua akses ke jaringan komputer hanya banyak dilakukan setelah melewati proses otentikasi. Proses otentikasi ini akan mengidentifikasi asal dan tujuan permintaan akses.
   2. Titik Akses ke jaringan BPKP harus disimpan pada ruangan tertutup yang hanya dapat diakses oleh pengelola jaringan. Titik akses jaringan yang tidak berada pada ruangan tertutup harus dilengkapi dengan mekanisme dan prosedur untuk mencegah penyalahgunaan titik akses tersebut.
   4. Pelanggaran otentikasi akan ditelusuri oleh pengelola jaringan dan dilaporkan kepada Pusinfowas untuk ditindaklanjuti sesuai ketentuan yang berlaku.
   5. Mekanisme otentikasi sekurangnya memenuhi :
      a. Validasi alamat asal dan permintaan
      b. Verifikasi pengamatan dan perangkat keras
      c. Pendeteksian duplikasi alamat.

D. Pengendalian Akses Jaringan Komputer
   1. Pengguna jaringan komputer mendapatkan hak akses minimal untuk melaksanakan tugas rutin.
   2. Pengaksesan ke jaringan LAN operasional dibatasi pada layanan *(service)* yang diperlukan saja.
   3. Semua jaringan dan peralatan jaringan komputer dikelola oleh pengelola jaringan komputer yang ditunjuk oleh Pusinfowas.
   4. Pengelola jaringan komputer bertanggung jawab dalam pengaturan dan pemantauan akses jaringan komputer dengan didukung oleh perangkat lunak pengelolaan jaringan yang memadai.

E. Hubungan dengan Jaringan Ekstemal
   1. Semua hubungan ke dan dari jaringan ekstemal harus dilengkapi dengan perangkat yang mampu melakukan pencatatan aktivitas yang terjadi pada jaringan komputer.
   2. Setiap konfigurasi hubungan jaringan komputer ke pihak eksternal harus mendapat persetujuan dari Kepala Pusinfowas dengan mempertimbangkan standar konfigurasi jaringan BPKP secara keseluruhan.
   3. Semua akses ke dan dari jaringan komputer BPKP hanya dapat dilakukan melalui perangkat keamanan jaringan BPKP yang sekurangnya memiliki kemampuan :
      a. Memastikan akses hanya dapat dilakukan ke alamat tujuan yang diperbolehkan.
      b. Mencegah akses ke alamat tujuan yang tidak diperbolehkan.
      c. Membatasi jenis layanan yang diperbolehkan ke alamat tujuan tertentu.
      d. Mencatat aktivitas akses ke jaringan komputer.

4. Pemanfaatan Public/*Share rounted network* untuk mengirim dan atau menerima data yang bersifat rahasia harus dilengkapi mekanisme pengamanan seperti pemanfaatan teknologi enkripsi.

VIII. PENGEMBANGAN PERANGKAT LUNAK

Kebijakan yang tercakup dalam bagian ini terdiri dari :
Kebijakan 1 : Permintaan Pengembangan Perangkat Lunak *(User Request)*
Kebijakan 2 : Pemenuhan Permintaan Pengembangan Perangkat Lunak
Kebijakan 3 : Pengendalian Mutu
Kebijakan 4 : Perangkat Lunak Pendukung
Kebijakan 5: Kepemilikan Perangkat Lunak
Kebijakan 6 : Implementasi Perangkat Lunak.
Lingkup Kebijakan :

- Kebijakan ini diberlakukan untuk seluruh pimpinan pegawai, dan mitra kerja
- BPKP.
- Kebijakan ini mencakup semua aspek yang terkait dengan tahapan pengembangan perangkat lunak.
- Pelanggaran atas kebijakan ini dapat mengakibatkan diberikannya sanksi-sanksi disipliner sesuai ketentuan yang berlaku di BPKP.

A. Permintaan Pengembangan Perangkat Lunak *(User Request)*
   1. Permintaan perangkat lunak diajukan secara tertulis kepada Pusinfowas setelah mendapat persetujuan dari pejabat/pimpinan unit kerja yang bersangkutan.
   2. Pusinfowas berkewajiban melakukan evaluasi teknis atas permintaan perangkat lunak dan menetapkan cara pemenuhan permintaan perangkat lunak, baik secara *inhouse, outsource,* atau pembelian "paket" perangkat lunak.
   3. Dalam hal timbul biaya untuk pemenuhan permintaan perangkat lunak, maka perlu dipastikan ketersediaan dananya.

B. Pemenuhan Permintaan Pengembangan Perangkat Lunak
   1. Pemenuhan permintaan pengembangan Perangkat Lunak sedapat mungkin dilakukan secara *inhouse.*
   2. Dalam hal pengembangan perangkat lunak dilakukan secara inhouse tidak memungkinkan, maka Pimpinan Unit Kerja di lingkungan BPKP melalui Kepala Pusinfowas dapat mengajukan usulan kepada Kepala BPKP untuk dilakukannya pengeml.angan perangkat lunak secara *outsourcing.*
   3. Pengembangan perangkat lunak melalui *outsourcing* dilakukan apabila memenuhi kondisi sebagai berikut :
      a. Tidak tersedia sumber daya manusia yang memiliki keahlian yang diperlukan untuk mengembangkan perangkat lunak tersebut.
      b. Tidak tersedia sumber daya manusia untuk memenuhi kerangka waktu yang diminta.
      c. Menyangkut hal-hal yang bersifat tidak strategis (rahasia perusahaan).
   4. Dalam hal permintaan perangkat lunak dipenuhi dengan cara *outsourcing* maka penunjukkan mitra kerja harus memperhatikan *:*
      a. Kemampuan dan pengalaman mitra kerja dalam membuat perangkat lunak yang diperlukan.
      b. Kemampuan untuk menyelesaikan perangkat lunak tepat waktu.
      c. Kemampuan memberikan dukungan purna jual *(after sales service)* dengan baik.
      d. Kemampuan memberikan solusi dengan biaya yang wajar.
   5. Untuk memastikan kualitas (mutu) perangkat lunak yang dihasilkan sesuai dengan permintaan pengguna, pengembangan perangkat lunak harus memenuhi ketentuan sebagai berikut :

a. Pengembangan perangkat lunak harus mengikuti prosedur dan metodologi pengembangan perangkat lunak yang ditetapkan oleh Kepala Pusinfowas.
b. Setiap perangkat lunak yang dibangun/dikembangkan wajib melalui proses pengendalian mutu.
c. Pengendalian mutu dilakukan oleh suatu Tim Pengendali Mutu yang sekurang-kurangnya terdiri dan wakil pemohon/pengguna dan wakil dari Pusinfowas.
d. Pengembangan perangkat lunak harus dilengkapi dengan dokumentasi pengembangan yang disetujui oleh Tim Pengenda1ian Mutu.
e. Pengendalian mutu dilakukan dengan mengacu kepada dokumen pengujian yang disiapkan oleh pengembang perangkat lunak.
f. Dokumen pengujian sekurang-kurangnya berisi rencana pengujian, prosedur pengujian fungsional, prosedur pengujian keamanan, prosedur unjuk kerja dan hasil pengujian.

C. Perangkat Lunak Pendukung
1. Pemilihan perangkat lunak pendukung pengembangan harus dikaji terlebih dahulu dan harus mendapat persetujuan Pusinfowas.
2. Perangkat lunak dimaksud harus mengacu pada standar yang telah ditetapkan oleh Kepala Pusinfowas.

D. Kepemilikan Perangkat Lunak
1. Hak cipta atas perangkat lunak yang dikembangkan dengan cara *inhouse development* ada pada BPKP.
2. Perangkat lunak yang dikembangkan dengan cara *outsourcing* merupakan milik BPKP, kecuali dinyatakan lain dalam kontrak (*agreement)*.

E. Implementasi Perangkat Lunak
1. Sebelum dilakukan implementasi perangkat lunak, pengembang perangkat lunak wajib melakukan pelatihan yang memadai bagi pemohon/calon penggunanya.
2. Dalam hal perangkat lunak tersebut digunakan untuk menggantikan perangkat lunak (maupun sistem secara manual) yang sudah ada sebelumnya, maka implementasinya harus melalui proses *parallel-run* selama tertentu untuk menghindari efek (risiko) kegagalan yang mungkin dari proses implementasi tersebut. Jika dipandang bahwa risiko kegagalan adalah relatif kecil dan tak sebanding dengan biaya impelementasi secara *parallel-run,* maka implementasi secara langsung *(direct impleme)* dapat ditempuh. Penetapan metode implementasi ini dilakukan Pusinfowas.
3. Pemindahan perangkat lunak aplikasi dan lingkungan pengembangan ke lingkungan produksi perlu dilaksanakan melalui prosedur yang ditetapkan, didokumentasikan, dan dilakukan oleh pihak yang berwenang, dengan memperhatikan prosedur cadangan (*fallback procedure*) jika terjadi kegagalan.
4. Penggunaan perangkat lunak di lingkungan produksi hanya dapat dilakukan setelah disetujui oleh Pimpinan / Pejabat unit kerja yang me pengembangan perangkat lunak tersebut.
5. Evaluasi dan pemeliharaan perangkat lunak perlu dilakukan berkesinambungan untuk memastikan bahwa sistem yang diimplementasikan masih sesuai dan relevan dengan kebutuhan pengguna.
6. Kebutuhan akan perubahan perangkat lunak yang sudah beroperasi dilakukan sesuai prosedur yang ditetapkan oleh Kepala Pusinfowas.

IX. DISASTER RECOVERY PLAN

Kebijakan yang tercakup dalam bagian ini terdiri dari :
Kebijakan 1 : Kondisi *Disaster*
Kebijakan 2 : Penetapan Kondisi *Disaster*
Kebijakan 3 : Keselamatan Jiwa dalam Kondisi *Disaster*
Kebijakan 4 : Organisasi Tim Pemulihan Kondisi *Disaster*
Kebijakan 5 : Pemulihan Data dan Sistem
Kebijakan 6 : Prosedur Pemulihan dan Uji Coba Prosedur
Kebijakan 7 : Lokasi Pemulihan
Lingkup Kebijakan :

- Kebijakan ini diberlakukan untuk seluruh pimpinan, pegawai, dan mitra kerja BPKP.
- Kebijakan ini mencakup semua aspek mengenai Rencana Pemulihan Data dan Sistem BPKP pada kondisi darurat (BPKP's *D,saster Recovery Plan)*
- Pelanggaran atas kebijakan ini dapat mengakibatkan diberikannya sanksi-sanksi disipliner, sesuai ketentuan yang berlaku di BPKP.

A. Kondisi Disaster
   1. Setiap karyawan, pejabat ataupun pimpinan BPKP yang mengetahui terjadinya kondisi *disaster* di atas wajib memberitahukan kondisi disaster tersebut kepada Pusinfowas.
   2. Dalam kondisi *disaster* Pusinfowas dapat melakukan hal-hal yang dianggap perlu untuk melindungi aset BPKP di Pusat Data.

B. Penetapan Kondisi Disaster
   1. Kondisi *disaster* wajib diajukan oleh Kepala Pusinfowas atau pihak lain yang ditunjuk, untuk dikonsultasikan dan mendapat persetujuan penanganan dari Kepala BPKP.
   2. Penetapan kondisi *disaster* dilakukan oleh Kepala BPKP.
   3. Dalam hal Kepala BPKP berhalangan, maka penetapan kondisi *disaster* dapat dilakukan oleh Sekretaris Utama atau salah satu Deputi BPKP.

C. Keselamatan Jiwa dalam Kondisi Disaster
   1. Dalam kondisi *disaster* keselamatan jiwa karyawan BPKP adalah hal yang harus diutamakan dan mendapatkan prioritas pertama.
   2. Kegiatan yang dilakukan selama kondisi *disaster* tetap mempertimbangkan keselamatan jiwa dan mengikuti ketentuan-ketentuan yang ditetapkan oleh Tim Pengendalian Keadaan Darurat BPKP.

D. Organisasi Tim Pengendalian Keadaan Darurat
   1. Tim Pengendalian Keadaan Darurat terdiri dari :
      a. Kepala Pusinfowas sebagai Ketua Tim;
      b. Seluruh pejabat struktural di Pusinfowas ;
      c. Staf / pegawai BPKP yang ditunjuk sebagai Kustodi Data dan Sistem;
      d. Pejabat Eselon II, III, dan IV dari unit kerja pengguna sistem yang akan dipulihkan;
      e. Staf / pegawai BPKP lainnya yang dianggap perlu.
   2. Tim Pengendalian Keadaan Darurat dipimpin oleh Kepala Pusinfowas dan mulai bekerja pada saat kondisi *disaster* ditetapkan.
   3. Ketua Tim Pengendalian Keadaan Darurat mempunyai tugas :
      a. Menentukan waktu, tempat, dan pelaku pelaksanaan pemulihan.
      b. Mengkoordinasikan dan memonitor pelalLsanaan pemulihan
      c. Melaporkan aktivitas pemulihan kepada Kepala BPKP.

E. Pemulihan Data dan Sistem
1. Tim Pengendalian Keadaan Darurat wajib memulihkan seluruh sistem utama BPKP di lokasi pemulihan dalam jangka secepatnya, dan sedapat mungkin tidak lebih dari 2 kali 24 jam sejak dinyatakannya kondisi *disaster.*
2. Tim Pengendalian Keadaan Darurat akan memulihkan data dari sistem utama BPKP di lokasi pemulihan sesuai kondisi *backup* system atau data terakhir.
3. Salah satu pejabat (sekurang-kurangnya Eselon II) dari unit kerja pengguna sistem bertugas melakukan pemeriksaan atas kebenaran hasil proses pemulihan data dan sistem yang terkait.
4. Ketua Tim Pengendalian Keadaan Darurat wajib melakukan pemeriksaan atas kesiapan lokasi sebelum menggunakan atau mengoperasikan sistem atau data *backup.*
5. Pencabutan penetapan kondisi *disaster* serta keputusan untuk menggunakan atau mengoperasikan sistem secara normal dilakukan oleh Kepala BPKP atas usulan dari Ketua Tim Pengendalian Keadaan Darurat,

F. Prosedur Pemulihan dan Uji Coba Prosedur
1. Pengelola sistem utama BPKP wajib memiliki prosedur pemulihan sistem dan data, serta wajib menyampaikannya kepada Pusinfowas untuk disetujui.
2. Pengelola sistem utama BPKP wajib menyediakan segala sesuatu yang terkait dengan kelancaran proses pemulihan sistem dan data sesuai dengan prosedur yang disetujui.
3. Pengelola sistem utama BPKP wajib melaksanakan uji coba terhadap prosedur pemulihan sistem dan data sekurang-kurangnya dua kali dalam setahun, dan hasilnya dilaporkan kepada Pusinfowas.

G. Lokasi Pemulihan
1. Pengelola sistem utama BPKP wajib menyiapkan lokasi pemulihan dan infrastruktur sistem utama yang diperlukan untuk keperluan pemulihan system dan data pada kondisi *disaster.*
2. Persiapan dan pemeliharaan lokasi pemulihan serta infrastruktur yang diperlukan dapat dipenuhi dengan cara menggunakan jasa pihak ketiga (*outsourcing)*.r
3. Dalam keadaan dimana lokasi pemulihan yang telah dipersiapkan tidak dapat digunakan pada saat kondisi disaster, maka Ketua Tim Pengendalian Keadaan Darurat dapat mengusulkan lokasi pemulihan lainnya.
4. Lokasi pemulihan ditetapkan oleh Kepala BPKP berdasarkan usulan dari Kepala Pusinfowas.

X. KEBIJAKAN LAIN-LAIN

Kebijakan yang tercakup dalam bagian ini terdiri dari :
Kebijakan 1 : Sistem PBX
Kebijakan 2 : Voice Mail
Kebijakan 3 : Perlengkapan Personal Computer (PC)
Kebijakan 4 : Sistem Faksimili
Kebijakan 5 : Penyimpanan Dokumen Elektronik
Lingkup Kebijakan :
- Kebijakan ini diberlakukan untuk seluruh pimpinan, pegawai, dan mitra kerja BPKP.
- Kebijakan ini mencakup selurun perangkat keras komputer dan telekomunikasi yang mendukung kegiatan perkantoran di BPKP.
- Pelanggaran atas kebijakan ini dapat mengakibatkan diberikannya sanksi-sanksi disipliner, sesuai ketentuan yang berlaku di BPKP.

A. Sistem PBX
1. Sistem PBX hanya dipergunakan untuk kepentingan BPKP.

2. Sistem PBX mencatat waktu pembicaraan, nomor telepon dan jenis sambungan ke telepon publik dari seluruh sambungan telepon di lingkungan BPKP, dan akan dilaporkan secara berkala kepada Sekretaris Utama (SESMA) BPKP.
3. Perangkat sistem PBX dan pendukungnya harus diletakkan pada ruangan khusus yang aman dari pihak-pihak yang tidak berkepentingan.
4. Pesawat telepon yang terpasang di lokasi umum BPKP (seperti ruang rapat, ruang tunggu tamu, resepsionis, dan dapur) hanya dapat digunakan untuk komunikasi internal atau terbatas sesuai ketentuan Biro Umum dan perlengkapan BPKP.
5. Password administrasi PBX harus segera diganti setelah instalasi sistem PBX selesai dan diserahkan kepada petugas yang ditunjuk, untuk selanjutnya *password* tersebut harus diubah secara berkala.
6. Pesawat telepon milik BPKP tidak dapat dipindahkan tanpa persetujuan atau izin tertulis dari Kepala Biro Umum dan Perlengkapan sesuai ketentuan yang berlaku.
7. Pusinfowas bertugas menjamin kapasitas fasilitas PBX sehingga rasio keberhasilan panggil (*call success ratio)* pada sistem PBX tersebut mendekati 100%.
8. Pusinfowas bekerjasama Biro Umum dan Perlengkapan berkewajiban memelihara sistem PBX yang pelaksanaannya dapat dilakukan oleh pihak ketiga *(outsourcing)*.

B. Voice Mail
1. Voice Mail merupakan fasilitas tambahan (optional) dari sistem PBX BPKP yang diberikan sesuai kapasitas yang tersedia.
2. Voice Mail tidak secara otomatis diaktifkan pada saat penambahan ekstension, melainkan harus melalui permintaan secara tertulis sesuai prosedur dan ketentuan yang berlaku.
3. Seluruh akses ke Voice Mail harus dilindungi dengan PIN yang hanya boleh digunakan oleh pemiliknya.
4. *Password* administrator Voice Mail harus segera diganti setelah instalasi sistem PBX selesai dan diserahkan kepada petugas yang ditunjuk, untuk selanjutnya *password* tersebut harus diubah secara berkala.
5. Sedapat mungkin PIN untuk Voice Mail dibedakan dari PIN untuk fasilitas lain dalam sistem PBX.
6. Akses ke jalur telepon publik tidak dimungkinkan melalui fasilitas Voice Mail.
7. Penyebaran pesan kepada seluruh Voice Mail secara serentak tidak diperkenankan di lingkungan PBX BPKP.

C. Perlengkapan Personal Komputer
1. Pusinfowas wajib memberikan dukungan teknis terhadap masalah yang berkaitan dengan penggunaan PC *(Personal Computer)* dan perangkat pendukungnya untuk kelancaran dan pekerjaan di BPKP.
2. Perubahan perangkat keras pendukung PC harus dikoordinasikan kepada Pusinfowas.
3. Semua kontrak pemeliharan perangkat PC dan perangkat pendukungnya harus mendapatkan persetujuan dari Kepala Pusinfowas.
4. Pusinfowas tidak bertanggung jawab terhdaap pemeliharaan PC dan atau perangkat pendukung milik pribadi, atau yang dilakukan tanpa sepengetahuan dan koordinasi dengan Pusinfowas.
5. PC dan perangkat pendukung milik BPKP tidak dapat dipindahkan tanpa persetujuan dari Pusinfowas dan atau Biro Umum dan Perlengkapan sesuai ketentuan yang berlaku.

D. Sistem Faksimili

1. Perangkat faksimili di lingkungan BPKP harus dapat memberikan konfirmasi atau bukti pengiriman dan atau penerimaan.
2. Perangkat faksimili di lingkungan BPKP harus dikonfigurasikan dengan benar sehingga setiap penggunaan faksimili melalui perangkat tersebut dapat memberikan identitas yang benar, meliputi sekurang-kurangnya: nama mesin, lokasi, dan nomor jalur telepon yang digunakan.
3. Fasilitas faksimili harus dikonfigurasikan dengan benar untuk menghindari kemungkinan penyalahgunaan yang dapat mengganggu sistem di lingkungan BPKP.
4. Jalur telepon yang digunakan untuk fasilitas faksimili tidak diperbolehkan untuk keperluan mengakses jaringan komputer.
5. Peletakan fasilitas faksimili di daerah terbatas *(restricted area)* ditentukan oleh pengguna (sekurang-kurangnya Pejabat Eselon III) dengan mempertimbangkan tingkat kerahasiaan informasi yang akan diterima atau dikirim melalui fasilitas tersebut.
6. Semua pengiriman faksimili hams mencantumkan peryataan disclaimer yang sekurangnya berisi sebagai berikut :
   This fax is intended only for the use of the addressee named above and may contain confidential information. If you are not the addressee, we apologize for any inconvenience to you. Please telephon us immediately and we will arrange with you for retum of this fax at our expense. You should not copy this fax or rely on it or disclose it to any other person. To do this may be illegal.
7. Pengiriman faksimili yang berisi data Sangat Rahasia, Rahasia dan Konfidensial, tidak diperkenankan menggunakanjasa pengiriman faksimili melalui pihak ketiga.

E. Pemeliharaan Dokumen Elektronik

Semua dokumen elektronik akan disimpan dan dipelihara sesuai dengan kategori waktu yang akan diatur lebih lanjut dalam ketentuan kearsipan.

Ditetapkan di Jakarta
pada tanggal 17 April 2003
KEPALA BADAN PENGAWASAN
KEUANGAN DAN PEMBANGUNAN,
ttd.
ARIE SOELENDRO