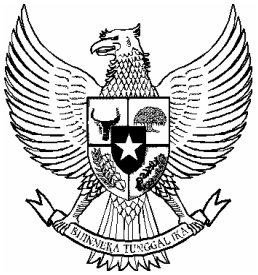


BERITA NEGARA REPUBLIK INDONESIA

No.558, 2014 BNPB. Teknologi Informasi. Kebencanaan. Pengelolaan. Pedoman.

PERATURAN KEPALA BADAN NASIONAL PENANGGULANGAN BENCANA
NOMOR 8 TAHUN 2014
TENTANG
PEDOMAN PENGELOLAAN TEKNOLOGI INFORMASI KEBENCANAAN

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN NASIONAL PENANGGULANGAN BENCANA,

Menimbang : a. bahwa untuk melaksanakan ketentuan Pasal 2 Peraturan Pemerintah Nomor 21 Tahun 2008 tentang Penyelenggaraan Penanggulangan Bencana, perlu dibuat Peraturan Kepala Badan Nasional Penanggulangan Bencana tentang Pedoman Pengelolaan Teknologi Informasi Kebencanaan;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Kepala Badan Nasional Penanggulangan Bencana tentang Pedoman Pengelolaan Teknologi Informasi Kebencanaan;

Mengingat : 1. Undang-Undang Nomor 24 Tahun 2007 tentang Penanggulangan Bencana (Lembaran Negara Republik Indonesia Tahun 2007 Nomor 66, Tambahan Lembaran Negara Republik Indonesia Nomor 4723);

2. Peraturan Pemerintah Nomor 21 Tahun 2008 tentang Penyelenggaraan Penanggulangan Bencana (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 43, Tambahan Lembaran Negara Republik Indonesia

Nomor 4828);

3. Peraturan Presiden Nomor 8 Tahun 2008 tentang Badan Nasional Penanggulangan Bencana;
4. Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan Elektronik Pemerintah;
5. Peraturan Kepala Badan Nasional Penanggulangan Bencana Nomor 1 Tahun 2008 tentang Organisasi dan Tata Kerja Badan Nasional Penanggulangan Bencana;
6. Peraturan Kepala Badan Nasional Penanggulangan Bencana Nomor 3 Tahun 2008 tentang Pedoman Pembentukan Badan Penanggulangan Bencana Daerah;
7. Peraturan Kepala Badan Nasional Penanggulangan Bencana Nomor 8 Tahun 2010 tentang Standardisasi Data Kebencanaan;
8. Peraturan Kepala Badan Nasional Penanggulangan Bencana Nomor 7 Tahun 2012 tentang Pengelolaan Data dan Informasi;

MEMUTUSKAN:

Menetapkan : PERATURAN KEPALA BADAN NASIONAL PENANGGULANGAN BENCANA TENTANG PEDOMAN PENGELOLAAN TEKNOLOGI INFORMASI KEBENCANAAN.

Pasal 1

Pedoman Pengelolaan Teknologi Informasi Kebencanaan merupakan panduan bagi Badan Nasional Penanggulangan Bencana dan Badan Penanggulangan Bencana Daerah agar pemanfaatan teknologi informasi kebencanaan dapat digunakan secara efektif dan efisien.

Pasal 2

Pedoman Pengelolaan Teknologi Informasi Kebencanaan sebagaimana dimaksud dalam Pasal 1 merupakan lampiran dan bagian yang tidak terpisahkan dari peraturan ini.

Pasal 3

Pedoman Pengelolaan Teknologi Informasi Kebencanaan disusun dengan Sistematika Sebagai Berikut :

BAB I PENDAHULUAN

BAB II TEKNOLOGI INFORMASI KEBENCANAAN

BAB III KEBIJAKAN UMUM TEKNOLOGI INFORMASI

BAB IV KEBIJAKAN PENGELOLAAN KOMPONEN TEKNOLOGI INFORMASI

BAB V KEBIJAKAN PENGELOLAAN APLIKASI SISTEM INFORMASI

BAB VI KEBIJAKAN KEAMANAN TEKNOLOGI INFORMASI

BAB VII PELAPORAN

BAB VIII PENUTUP

DAFTAR LAMPIRAN

Pasal 4

Peraturan Kepala Badan Nasional Penanggulangan Bencana ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan peraturan Kepala Badan Nasional Penanggulangan Bencana ini dengan penempatannya dalam berita negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 8 April 2014
KEPALA BADAN NASIONAL
PENANGGULANGAN BENCANA,

SYAMSUL MAARIF

Diundangkan di Jakarta
pada tanggal 24 April 2014
MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

AMIR SYAMSUDIN

BAB I
PENDAHULUAN

1.1. Latar Belakang

Negara Indonesia merupakan negara yang berada di wilayah rawan bencana. Kerawanan bencana ini ditandai dengan banyaknya bencana yang terjadi seperti gempa bumi, tsunami, letusan gunung api, banjir, tanah longsor, angin puting beliung, kekeringan, kebakaran hutan dan lahan, kegagalan teknologi, serta konflik sosial yang mengakibatkan korban jiwa manusia, kerusakan lingkungan, kerugian harta benda dan dampak psikologis. Sesuai dengan amanat Undang-Undang No.24 Tahun 2007 tentang Penanggulangan Bencana, disebutkan bahwa pemerintah Indonesia dalam hal ini pemerintah pusat dan pemerintah daerah bertanggung jawab dalam penyelenggaraan penanggulangan bencana, mulai dari tahap pra bencana, saat bencana sampai dengan pasca bencana.

Dengan infrastruktur teknologi informasi yang dimiliki sejak tahun 2010, BNPB telah membangun sebuah aplikasi sistem informasi kebencanaan terpadu untuk mendukung semua proses informasi dan data kebencanaan. BNPB juga telah banyak melakukan pemberian bantuan kepada BPBD secara berkesinambungan berupa kelengkapan perangkat teknologi informasi, seperti perangkat keras, perangkat lunak, serta perangkat jaringan komunikasi data untuk kebutuhan infrastruktur, sarana dan prasarana lainnya.

1.2. Maksud dan Tujuan

Maksud dari Peraturan Kepala BNPB ini adalah agar semua pengguna baik di BNPB dan BPBD Provinsi/Kabupaten/Kota dan juga bagi pengguna lain yang memiliki hubungan kerjasama dengan BNPB dan BPBD dapat menggunakan sumber daya teknologi informasi secara optimal, tepat dan akurat serta meningkatkan profesionalisme kerja seluruh karyawan dalam melakukan pengelolaan data dan informasi kebencanaan.

Tujuan dari Peraturan Kepala BNPB ini adalah untuk memastikan pengelolaan yang baik dan benar terhadap seluruh penggunaan sumber daya infrastruktur teknologi, sistem informasi dan data kebencanaan di lingkungan BNPB dan BPBD.

1.3. Ruang Lingkup dan Sasaran

Ruang lingkup Peraturan Kepala BNPB ini mencakup pada lingkungan BNPB dan seluruh BPBD Provinsi/Kabupaten/Kota dalam mempergunakan infrastruktur teknologi informasi kebencanaan yang disediakan oleh BNPB dan BPBD.

Sasaran dari Peraturan Kepala BNPB ini adalah meliputi seluruh pengguna dan pengelola teknologi informasi yang ada di lingkungan BNPB dan BPBD Provinsi/Kabupaten/Kota.

1.4. Pengertian

Beberapa istilah dan pengertian umum yang didefinisikan dalam Peraturan Kepala Pengelolaan Teknologi Informasi BNPB ini adalah sebagai berikut.

1. Sistem informasi adalah serangkaian perangkat dan prosedur komputasi yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi;
2. Sistem Informasi Kebencanaan Terpadu adalah sebuah perangkat lunak sistem informasi kebencanaan yang terpadu dan terpusat yang disediakan oleh BNPB dan dipergunakan untuk pengolahan data bencana baik prabencana, saat bencana dan pascabencana serta proses analisa data untuk pengambilan keputusan;
3. Badan Nasional Penanggulangan Bencana, yang selanjutnya disingkat dengan BNPB, adalah lembaga pemerintah non kementrian sesuai dengan ketentuan peraturan perundang-undangan;
4. Badan Penanggulangan Bencana Daerah, yang selanjutnya disingkat BPBD, adalah badan pemerintah daerah yang melakukan penyelenggaraan penanggulangan bencana di daerah.

1.5. Landasan Hukum

Pedoman Pengelolaan Teknologi Informasi Kebencanaan merujuk pada beberapa peraturan perundang-undangan sebagai berikut.

1. Undang-Undang Nomor 24 Tahun 2007 tentang Penanggulangan Bencana;
2. Peraturan Pemerintah Nomor 21 Tahun 2008 tentang Penyelenggaraan Penanggulangan Bencana;
3. Peraturan Presiden Nomor 8 Tahun 2008 tentang Badan Nasional Penanggulangan Bencana;
4. Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan Elektronik Pemerintah.
5. Peraturan Kepala BNPB Nomor 1 Tahun 2008 tentang Organisasi Dan Tata Kerja Badan Nasional Penanggulangan Bencana;
6. Peraturan Kepala BNPB Nomor 3 Tahun 2008 tentang Pedoman Pembentukan Badan Penanggulangan Bencana Daerah;
7. Peraturan Kepala BNPB Nomor 8 Tahun 2010 tentang Standardisasi Data Kebencanaan;
8. Peraturan Kepala BNPB Nomor 7 Tahun 2012 tentang Pengelolaan Data dan Informasi;

BAB II
TEKNOLOGI INFORMASI KEBENCANAAN

Teknologi informasi adalah sekumpulan komponen yang terdiri dari perangkat keras, perangkat lunak, data, proses dan servis yang digunakan sebagai proses pengambilan keputusan. Teknologi informasi kebencanaan merupakan keseluruhan proses pengolahan data dan informasi kebencanaan yang didukung oleh sumber daya dan infrastruktur teknologi informasi yang ada di BNPB dan BPBD.

2.1. Kebijakan dan Strategi

Kebijakan yang diambil dalam pengelolaan teknologi informasi di BNPB dan BPBD adalah sebagai berikut.

1. Teknologi informasi harus dikelola secara efektif dan efisien agar dapat berjalan dengan baik karena penting dalam mendukung proses pengambilan keputusan bagi BNPB dan BPBD;
2. Teknologi informasi harus diimplementasikan secara terpadu dan terarah agar proses pengelolaan data dan proses analisis informasi menjadi lebih mudah sehingga penanganan bencana lebih efektif dan efisien.

Untuk mendukung kebijakan teknologi informasi, maka strategi teknologi informasi BNPB dapat diuraikan sebagai berikut.

1. BNPB dapat memanfaatkan infrastruktur secara optimal sesuai dengan kondisi terkini;
2. BNPB memiliki payung hukum Peraturan Kepala (PERKA) dan Petunjuk Teknis (JUKNIS) yang lengkap dari keseluruhan komponen infrastruktur;
3. BNPB dapat mengoptimalkan semua sumber daya tenaga pengelola teknologi informasi baik di BNPB maupun di BPBD dan menyediakan bimbingan teknis yang cukup bagi seluruh pengguna aplikasi kebencanaan;
4. BNPB memiliki aplikasi pendukung sistem kebencanaan yang terpadu, terintegrasi satu dengan lainnya, dalam serambi sistem operasi dan basis data yang sama atau melalui konsep basis data satu pintu;
5. BNPB dan BPBD memiliki standarisasi perangkat dan komponen teknologi dan mengadopsi standar keamanan teknologi informasi yang terkini;
6. BNPB dapat menerapkan Elektronik Pemerintah guna meningkatkan pelayanan publik dan transparansi.

2.2. Organisasi

Sistem organisasi BNPB telah diatur di dalam Peraturan Kepala BNPB Nomor 1 tahun 2008 tentang Organisasi dan Tata kerja BNPB yang menyebutkan bahwa tugas pokok Pusat Data Informasi dan Humas adalah "melaksanakan pengkoordinasian pengelolaan data dan informasi, pengembangan basis data dan sistem informasi, serta pelaksanaan hubungan masyarakat di bidang penanggulangan bencana". Dengan demikian pengelolaan sistem informasi kebencanaan di tingkat nasional termasuk infastruktur teknologinya dilakukan oleh Pusat Data, Informasi dan Humas.

Untuk pengaturan di daerah, pengelolaan data dan informasi di tingkat Provinsi ataupun Kabupaten dilakukan oleh sekretariat BPBD Provinsi/Kabupaten/Kota, ini sesuai dengan Peraturan Kepala BNPB Nomor 3 Tahun 2008 tentang Pedoman Pembentukan BPBD.

2.3. Tata Kerja

Mekanisme tata kerja pengelolan teknologi informasi di BNPB dan BPBD dapat diuraikan sebagai berikut.

1. Pengelola Teknologi Informasi BNPB bertanggung jawab untuk menyediakan infrastruktur dan aplikasi teknologi informasi yang dibutuhkan untuk tingkat nasional, serta memastikan bahwa infrastruktur dan aplikasi dapat berjalan dengan baik serta dapat mengikuti perkembangan organisasi dan perkembangan teknologi yang ada;
2. Staf pengelola teknologi informasi BPBD sesuai daerahnya masing-masing berfungsi untuk membantu menyelesaikan permasalahan umum seperti permasalahan komputer dan jaringan termasuk juga melakukan pengawasan dan pemeliharaan terhadap semua peralatan teknologi seperti peralatan radio komunikasi dan mobil komunikasi, menggunakan aplikasi teknologi informasi sesuai juknis penggunaannya serta memberikan laporan kepada Sekretariat BPBD masing-masing;
3. Semua permasalahan terkait teknologi informasi di BPBD yang tidak dapat diselesaikan dapat meminta bantuan dukungan dan bimbingan teknis kepada pengelola teknologi informasi BNPB melalui Sekretaris di wilayah / areanya masing-masing;

2.4. Sumber Daya

Terdapat lima sumber daya yang terlibat di dalam pengelolaan teknologi informasi kebencanaan di BNPB dan BPBD yang dijelaskan sebagai berikut.

1. Perangkat Keras

Perangkat keras merupakan sebuah komponen utama dalam mendukung sebuah aplikasi sistem informasi kebencanaan, dan penggunaan perangkat komunikasi untuk mendukung pekerjaan seperti radio komunikasi, mobil komunikasi. Kelengkapan perangkat keras pendukung sistem informasi kebencanaan dapat dilihat pada tabel dibawah ini.

Table 3.1.1 Sumber Daya Perangkat Keras

No	Kategori	Item	Deskripsi
1	Perangkat Keras	Rak Sistem Komputer	Rak Sistem Komputer
		Sistem Komputer	Sistem Komputer di instal pada rak
		Kabel	Kabel jaringan yang terhubung ke perangkat
		Basis Komputer Pribadi	Komputer Pribadi untuk operasional
		Genset	Sumber daya listrik cadangan
		Pembatas perangkat lunak	Perangkat jaringan yang terhubung dengan keamanan jaringan
		Mobil Komunikasi	Mobil Komunikasi dan Radio Komunikasi
		Satelit	Perangkat komunikasi ke satelit
	Perangkat Keras	Telepon Pintar	Perangkat Komunikasi melalui jalur tanpa kabel (GSM-CDMA)
		Alat untuk mengirim data	Komunikasi ke LAN dan WAN, Internet
2	Jaringan	WAN	Jaringan Area Besar terhubung keluar
		LAN	Tempat jaringan dan kabel jaringan dalam
3	Sumber Listrik Cadangan	Power Pembangkitan Listrik	Sumber listrik cadangan yang terhubung pada semua peralatan komponen teknologi informasi

2. Perangkat Lunak

Perangkat lunak merupakan penghubung antara perangkat keras dan pengguna. Perangkat lunak dalam sistem informasi kebencanaan dapat di klasifikasikan ke dalam dua bagian yakni:

a. Sistem perangkat lunak yaitu sistem yang berfungsi untuk mengontol penggunaan dan pengalokasian komponen perangkat keras dan program-program aplikasi lainnya yang digunakan. Tiga komponen sistem perangkat lunak adalah (a) Sistem Operasi, (b) Sistem Utiliti, (c) Sistem file yang dibutuhkan oleh sistem operasi dan aplikasi-aplikasi lainnya;

b. Aplikasi perangkat lunak yaitu perangkat lunak yang dibuat/dikembangkan menjadi sebuah aplikasi guna membantu pekerjaan secara spesifik dan menggunakan proses basis data. Aplikasi perangkat lunak diklasifikasikan sebagai berikut.

   - Aplikasi Kustomisasi yaitu aplikasi yang dirancang dan dikembangkan untuk kebutuhan pengelolaan data kebencanaan;
   - Aplikasi Paket yaitu aplikasi pendukung pekerjaan umum yang dikembangkan dan dijual oleh pengembang perangkat lunak;

3. Manusia

Sistem Informasi dapat berfungsi secara optimal bila sumber daya manusianya dapat menguasai penggunaan perangkat teknologi dan pemahaman proses dari operasional kebencanaan. Sumber daya manusia merupakan sebuah aset utama dalam proses transaksi sistem informasi. Persyaratan minimal yang harus dimilki bagi seorang staf/operator data dalam menggunakan dan mengolah sistem informasi kebencanaan di BNPB atau BPBD dijelaskan sebagai berikut.

a. Memilki otoritas terkait pekerjaannya sebagai operator data atau tenaga komputer di BNPB atau BPBD;

b. Memiliki kemampuan mengoperasikan komputer dan aplikasi paket yang digunakan dalam mengolah data-data kebencanaan, juga dapat menggunakan internet dan surat elektronik;

c. Mampu dan memahami seluruh alur proses pada sistem informasi kebencanaan;

d. Memahami Peraturan Kepala BNPB yang terkait pada unit tempat bekerja dan Peraturan Kepala BNPB lainnya secara umum.

4. Media Jaringan

Media komunikasi data dan informasi pada BNPB selain menggunakan media telepon, faksimili, jaringan internet dan satelit serta frekwensi radio. Basis aplikasi sistem informasi kebencanaan yang berjalan menggunakan jaringan intranet dan internet dan dapat diakses menggunakan modem melalui perangkat komunikasi, misal telepon pintar.

5. Data dan Informasi

Sistem Informasi kebencanaan di BNPB merupakan basis data dan informasi kebencanaan yang diorganisasikan untuk mengelola data bencana baik pra, saat bencana dan paca bencana menjadi kumpulan informasi yang dapat digunakan untuk memecahkan masalah dan proses pengambilan keputusan. Pengelolaan data dan informasi bencana meliputi pengumpulan, pengolahan, analisis, penyajian dan diseminasi informasi.

BAB III
KEBIJAKAN UMUM TEKNOLOGI INFORMASI

Kebijakan umum teknologi informasi dapat diklasifikasikan dalam empat belas kebijakan yang dijelaskan sebagai berikut.

1. Kebijakan Perencanaan Teknologi Informasi
2. Kebijakan Lisensi Perangkat Lunak
3. Kebijakan Elektronik-Pemerintah
4. Kebijakan Standarisasi Nama Dokumen
5. Kebijakan Penggunaan Grup Jaringan
6. Kebijakan Penggunaan Internet
7. Kebijakan Penggunaan Intranet
8. Kebijakan Penggunaan Surat Elektronik
9. Kebijakan Cadangan dan Pengembalian
10. Kebijakan Kontrol Perubahan
11. Kebijakan Dukungan Tenaga Komputer Untuk Pengguna
12. Kebijakan Penanganan Insiden dan Masalah
13. Kebijakan Manajemen Servis Level
14. Kebijakan Pengadaan Sistem dan Perangkat Teknologi Informasi

3.1. Perencanaan Teknologi Informasi

Tujuan kebijakan ini adalah untuk memastikan bahwa perencanaan teknologi informasi sejalan dan mendukung sepenuhnya terhadap kebutuhan BNPB dan BPBD saat ini dan di masa yang akan datang.

1. Ruang lingkup kebijakan ini mencakup area infrastruktur teknologi informasi pada BNPB dan BPBD;
2. Perencanaan teknologi informasi BNPB harus dituangkan ke dalam rencana jangka pendek dan jangka panjang dan harus sesuai dengan rencana strategis BNPB;
3. Perencanaan teknologi informasi di BPBD (jika sudah ada dan terbentuk) harus mengacu kepada perencanaan teknologi informasi di BNPB. Hal ini mencegah adanya tumpang tindih kebutuhan teknologi informasi antara BNPB dan BPBD;
4. Pengelola teknologi informasi BNPB bertanggung jawab untuk mengembangkan rencana kerja pengelolaan teknologi informasi yang dapat mendukung BNPB dalam pencapaian seluruh misi dan tujuannya;
5. Secara teratur, rencana kerja teknologi informasi harus ditinjau ulang dan disesuaikan terhadap perubahan kebutuhan dan kondisi teknologi informasi terkini;

6. Pengelola teknologi informasi BNPB harus menjaminkan terhadap proses rencana kerja yang tepat waktu dan akurat serta mengakomodasi perubahan atas rencana strategis BNPB dan perubahan kondisi teknologi informasi pada umumnya;
7. Perencanaan pengelolaan teknologi informasi harus memuat hal-hal sebagai berikut.
   a. dapat menelaah kemampuan sistem dan teknologi saat ini dan di masa yang akan datang;
   b. dapat memetakan proses utama teknologi informasi BNPB dimasa yang akan datang;
   c. dapat mendokumentasikan model dan standarisasi data di masa yang akan datang;
   d. dapat menentukan kebutuhan infrastruktur di masa depan sesuai dengan standar teknologi informasi BNPB;
   e. mendapat persetujuan dari pimpinan BNPB.
8. Seluruh pihak di BNPB baik di kedeputian dan atau bidang, jika memiliki usulan terhadap perencanaan teknologi informasi harus berkordinasi dengan Pusdatinmas BNPB. Kepada Pusdatinmas akan memberikan arahan dan panduan agar tetap sesuai dengan strategi teknologi yang sudah ditetapkan di BNPB;
9. Pengelola teknologi informasi BNPB dan BPBD bertanggung jawab untuk mematuhi kebijakan ini.

3.2. Lisensi Perangkat Lunak

Tujuan kebijakan ini adalah untuk memastikan kepatuhan pada ketentuan lisensi dari seluruh perangkat lunak yang dimiliki oleh BNPB dan BPBD. (Formulir ini dapat dilihat pada **lampiran 1**).

1. Ruang lingkup kebijakan ini mencakup semua perangkat lunak yang dipergunakan oleh BNPB termasuk sistem operasi, basis data dan perangkat lunak aplikasi;
2. Semua pembelian perangkat lunak harus disetujui oleh pimpinan pengelola teknologi BNPB atau BPBD diwilayah/areanya masing-masing;
3. Pengelola teknologi informasi harus memelihara dan mengamankan seluruh dokumentasi yang dibutuhkan untuk mendukung kepemilikan atas perangkat lunak;
4. Seluruh perangkat lunak harus dipergunakan sesuai dengan ketentuan yang ada di perjanjian lisensi;
5. Hanya pengelola teknologi informasi yang ditunjuk yang boleh melakukan instalasi perangkat lunak pada komputer dan atau perangkat berbasis komputer properti milik BNPB atau BPBD;
6. Pengguna dilarang mendistribusikan, menerima atau memiliki salinan yang tidak sah dari sebuah perangkat lunak yang tidak terdaftar

dalam Standar Lingkungan Operasi;

7. Pengguna dilarang menggunakan dan melakukan instalasi perangkat lunak tidak berlisensi (bajakan) dalam perangkat komputernya;
8. Pengguna yang melakukan instalasi perangkat lunak yang tidak berlisensi pada komputer harus mendapat persetujuan dari atasan pengguna dan pengelola teknologi, seperti melakukan instalasi perangkat lunak yang bersifat periode percobaan (masa percobaan maksimal 1 bulan) ataupun perangkat lunak yang terbuka. Hal ini menyangkut keamanan sistem operasi dan dampak virus terhadap sistem jaringan jika terjadi serangan luar yang tersembunyi dalam sebuah perangkat lunak;
9. Semua pengelola teknologi di BNPB dan BPBD bertanggung jawab untuk melakukan pemeriksaan perangkat lunak pada semua perangkat komputer secara berkala sebagai bukti kepemilikan perangkat lunak termasuk mencatat dan memperbaharui daftar perangkat lunak yang ber-lisensi;
10. Pengelola teknologi di BPBD membantu melaporkan semua perangkat lunak yang terinstal pada komputer di areanya kepada pengelola teknologi BNPB agar terjadi sinkronisasi standar perangkat yang sesuai dengan kebijakan pengelolaan teknologi informasi BNPB;
11. Seluruh pengguna komputer wajib untuk mematuhi kebijakan ini.

3.3. Elektronik_Pemerintah

Berdasarkan Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan elektronik-pemerintah adalah bertujuan untuk memperbaiki mutu pelayanan publik dengan mengelola dan pendayagunaan informasi dalam volume yang besar secara cepat dan akurat.

1. Pembentukan jaringan informasi dan transaksi pelayanan publik yang lebih transparan dan berguna bagi masyarakat, dalam hal ini BNPB dan BPBD memberikan informasi secara transparan dengan menggunakan teknologi sistem informasi yang terkait kebencanaan;
2. Pembentukan mekanisme dan saluran komunikasi dengan semua lembaga negara serta penyediaan fasilitas dialog publik, serta pembentukan sistem manajemen dan proses kerja yang transparan dan efisien serta memperlancar transaksi dan pelayanan antar lembaga pemerintah. Kebijakan ini akan memanfaatkan infrastruktur informasi teknologi yang ada di BNPB dan BPBD;
3. Pemanfaatan teknologi informasi secara optimal;
4. Pengembangan sumber daya manusia baik di pusat ataupun di daerah.

3.4. Standarisasi Nama Dokumen

Tujuan Standarisasi Nama Dokumen adalah untuk menetapkan standarisasi nama pada seluruh dokumen elektronik yang tersimpan di

dalam sistem komputer agar mudah dalam pengelolaannya dan lebih sesuai di dalam pengelompokan atas dokumen-dokumen yang lain.

1. Ruang lingkup kebijakan ini adalah mencakup seluruh dokumen elektronik khusus untuk dokumen informasi teknologi yang tersimpan di dalam sistem komputer di lingkungan BNPB dan BPBD seperti dokumen-dokumen aplikasi untuk Petunjuk Teknis (JUKNIS) dan lainnya;
2. Dokumen elektronik yang resmi untuk teknologi informasi harus memuat informasi sebagai berikut.
   a. Nama, yakni nama dokumen;
   b. Nomor, yakni nomor referensi atau nomor versi dokumen;
   c. Tanggal, yakni tanggal dokumen disetujui;
   d. Diperiksa Oleh, yakni yakni nama dan jabatan pemeriksa dokumen;
   e. Ruang Lingkup, yakni ruang lingkup informasi dalam dokumen;
   f. Disetujui Oleh, yakni nama dan jabatan staf yang menyetujui;

Contoh:

Nama:	Standar Operasional Prosedur. Kontrol Perubahan
Nomor:	v.01
Tanggal:	01 Januari 2013
Diperiksa Oleh:	Kepala Informasi BNPB
Ruang Lingkup:	BNPB, BPBD
Disetujui Oleh:	Kepala Informasi BNPB

3. Pengelola teknologi informasi bertanggung jawab untuk memastikan standar nama dokumen telah dapat dibuat/diaplikasikan pada seluruh dokumentasi teknologi yang dicatatnya;
4. Pengelola teknologi informasi harus menjelaskan kepada pengguna yang membutuhkan pengertian dan kejelasan tata cara membuat nama standar pada dokumen terkait dokumen informasi teknologi;
5. Seluruh pihak yang hendak membuat dokumen baru harus mematuhi kebijakan ini.

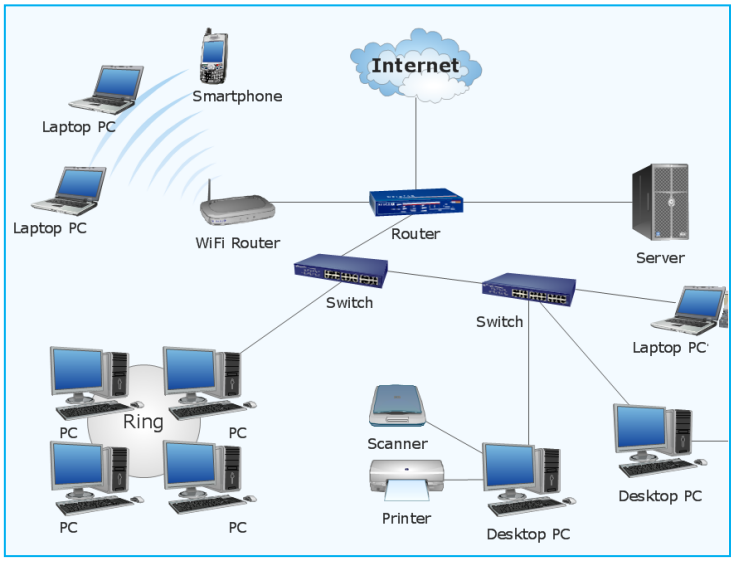
3.5. Penggunaan Grup Jaringan

Tujuan kebijakan ini adalah agar penggunaan jaringan internal teknologi informasi yang dikelola oleh BNPB atau BPBD hanya digunakan untuk keperluan pekerjaan yang terkait dengan kepentingan BNPB dan BPBD. Akses menggunakan jaringan lokal/luar pada BNPB dikelola dengan jaringan grup kerja dan penyesuaian penggunaan nama unik grup akan

dilakukan setelah kebutuhan rencana teknologi informasi ditetapkan. Perubahan akan di sosialisasikan kepada pengguna secara bertahap.

1. Ruang lingkup kebijakan ini adalah mengikat bagi seluruh pengguna teknologi jaringan di BNPB dan BPBD baik lokal atapun luar;
2. Akses GRUP KERJA masih dapat dipergunakan sampai dengan diputuskan kebijakan menggunakan NAMA UNIK bagi BNPB. Pengelola teknologi harus memastikan keamanan penggunaan setiap Protokol Internet DHCP atau Protokol Internet statis yang terpakai di sistem;
3. Akses disediakan sebagai penunjang pekerjaan pengguna jaringan dan harus digunakan hanya untuk kepentingan BNPB dan BPBD;
4. Pemasangan konfigurasi jaringan perangkat komputer dari pihak ketiga atau perangkat yang tidak dikelola oleh pengelola teknologi informasi maka harus dicatat dalam file. Pengaturan ini meliputi pencatatan alamat dan Protokol Internet statis jika diperlukan;
5. Semua pengguna komputer baru yang belum pernah terkoneksi ke dalam Jaringan Area Besar terhubung keluar harus melaporkan kepada staf teknologi informasi untuk segala kebutuhan koneksinya. Permintaan koneksi jaringan internal area luar terhubung keluar tersebut harus sepengetahuan dari atasan pengguna;
6. Pengelola teknologi harus memastikan keamanan komputer pengguna sebelum di daftarkan ke dalam daftar jaringan internal Jaringan Area Besar terhubung keluar di BNPB atau BPBD;
7. Pengelola teknologi harus memastikan perangkat lunak standar pada komputer pengguna;
8. Pengelola teknologi harus memastikan keamanan komputer pengguna (seperti virus dan lainnya) sebelum di daftarkan ke dalam daftar jaringan Jaringan Area Besar terhubung keluar di BNPB dan BPBD;
9. Pengelola teknologi dan seluruh pengguna jaringan dan atau pihak ketiga pengguna jaringan Jaringan Area Besar terhubung keluar dengan Nama Unik atau Grup Kerja yang berada di lingkungan BNPB dan BPBD bertanggung jawab untuk mematuhi kebijakan ini;
10. Pengelola teknologi akan menyesuaikan kebutuhan penggunaan grup ini dengan strategi teknologi informasi yang di tinjau ulang secara berkala;
11. Kebijakan penggunaan nama unik belum dapat dilaksanakan mutlak hingga kebijakan nama unik jaringan terhadap perubahan infrastruktur BNPB ditetapkan, namun demikian pengelolaan grup jaringan tetap menjadi tanggung jawab bagi pengelola teknologi informasi.

Standar desain jaringan dapat dilihat pada gambar berikut.



Gambar 3.5.1 Grup Jaringan

3.6. Penggunaan Internet

Tujuan kebijakan ini adalah untuk memastikan bahwa akses internet adalah hanya untuk kepentingan pekerjaan di lingkungan BNPB dan BPBD.

1. Ruang lingkup kebijakan ini berlaku untuk pengguna internet di BNPB dan BPBD dan atau pihak ketiga yang yang berkepentingan dengan BNPB atau BPBD dalam menggunakan jaringan internet;
2. Seluruh akses internet disediakan sebagai salah satu perangkat penunjang yang digunakan hanya untuk kepentingan resmi BNPB dan BPBD;
3. Pengguna internet untuk kepentingan pribadi diperbolehkan namun terbatas. Penggunaan tersebut, harus rasional dan tidak boleh mengganggu pekerjaan staf tersebut atau staf lain;
4. Penggunaan perangkat selain komputer (misal telepon pintar dan lainnya) yang digunakan untuk mengakses internet harus sepengetahuan staf pengelola teknologi. Dokumentasi log tersebut dicatat dalam sistem akses;
5. Pengguna internet dilarang mengakses pengambilan file ataupun mencetak bahan-bahan yang bersifat tidak etis dan menginformasikan apapun yang sifatnya menyerang jenis kelamin, ras, atau cacat tubuh tertentu, termasuk dilarang berpartisipasi dalam perjudian secara langsung;
6. Akses internet harus dikelompokan bagi pengguna di luar karyawan BNPB atau BPBD dengan menggunakan masuk akses dan kata kunci, hal ini untuk memastikan rekaman pengguna. Hal ini diatur dalam sistem tempat penyimpanan komputer;
7. Pengelola teknologi BNPB harus memiliki sistem jejak dikelompokkan dari akses ke internet yang dilakukan pengguna, hal ini

meminimalkan faktor keamanan dari penggunaan jaringan internet;

8. Pengelola teknologi informasi BNPB dan BPBD bertanggung jawab terhadap pengelolaan dan keamanan internet;
9. Seluruh pengguna internet dan atau pihak ketiga yang berkepentingan dengan BNPB atau BPBD harus mematuhi kebijakan ini.

3.7. Penggunaan Intranet

Tujuan kebijakan ini adalah untuk memastikan bahwa akses intranet adalah hanya untuk kepentingan pekerjaan di BNPB dan BPBD.

1. Ruang lingkup kebijakan ini berlaku untuk seluruh pengguna intranet di BNPB dan BPBD dan juga kepada pihak ketiga yang terikat kerjasama dengan BNPB atau BPBD dalam menggunakan infrastruktur Intranet di lingkungan jaringan BNPB dan BPBD.
2. Informasi harus sesuai untuk website dan sesuai dengan tujuan intranet.
3. Isi informasi Intranet harus singkat menggunakan bahasa yang sederhana, informatif dan jelas serta berguna bagi kepentingan BNPB dan BPBD.
4. Isi informasi Intranet harus berorientasi pada tindakan/keputusan. dan harus selalu terbaru.

5. Intranet harus memiliki keamanan akses dari pengguna publik diluar BNPB dan BPBD.
6. Isi informasi Intranet tidak boleh meniru konten pada web publik atau meniru konten yang telah disebarluaskan dan dikomunikasikan melalui cara lain (misalnya mempublikasikan elketronik surat atau koran staf). Hal ini untuk menghindari yang duplikasi. Pengecualian termasuk dokumen/arsip di BNPB dan BPBD.
7. Pengelola teknologi informasi BNPB bertanggung jawab terhadap pengelolaan pengembangan dan keamanan intranet.
8. Seluruh pengguna Intranet dan atau pihak ketiga yang berkepentingan dengan BNPB dan BPBD harus mematuhi kebijakan ini.
9. Intranet wajib digunakan setelah semua persiapan aplikasi sistem intranet telah dibuat dengan sempurna dan sudah menjadi standar aplikasi intranet BNPB.

3.8. Penggunaan Surat elektronik

Tujuan kebijakan ini adalah untuk memastikan layanan surat elektronik digunakan hanya untuk mendukung pekerjaan di BNPB dan BPBD.

1. Ruang lingkup kebijakan ini adalah mengikat bagi seluruh pengguna akun surat elektronik yang didaftarkan dalam nama unik surat elektronik BNPB. Untuk penggunaan surat elektronik diluar nama unik@bnpb.go.id masih diperkenankan dengan tetap mentaati peraturan etika umum surat elektronik pada kebijakan ini;
2. Sistem surat elektronik harus dipergunakan secara bertanggung jawab untuk tujuan yang berkaitan dengan pekerjaan BNPB atau BPBD;
3. Fasilitas surat elektronik tidak dianjurkan untuk menggantikan komunikasi tatap muka saat komunikasi lisan jelas-jelas lebih layak dilakukan;
4. Pengguna surat elektronik adalah semua karyawan atau Pegawai Negeri Sipil yang masih aktif bekerja di BNPB atau BPBD yang telah terdaftar dalam sistem akun surat elektronik pada jaringan nama unik BNPB;
5. Pengguna bertanggung jawab atas surat elektronik yang dikirim melalui alamat surat elektroniknya. Kata kunci harus digunakan setiap waktu dan pengguna disarankan untuk keluar dari sistem surat elektronik saat tidak dipergunakan;
6. Pengguna harus memastikan keamanan id pengguna dan kata kunci yang diberikan kepadanya;
7. Pengguna disarankan agar menggunakan fasilitas diluar kantor pada sistem surat elektronik saat pengguna tersebut tidak masuk kantor untuk jangka waktu tertentu;
8. Pengguna diperkenankan mengirim surat elektronik jika informasi

yang dikirim relevan bagi penerimanya;

9. Pengguna harus berhati-hati dalam menggunakan daftar alamat surat elektronik daftar untuk memastikan surat elektronik diterima orang-orang yang tepat;
10. Pengguna harus mempergunakan standar norma kesopanan dan profesionalisme seperti dalam komunikasi tertulis dan lisan;
11. Pengguna harus melakukan pembersihan/penghapusan box surat surat elektronik secara teratur dan surat elektronik hanya disimpan (cadangan) jika memang dibutuhkan;
12. Pengguna harus memastikan bahwa replikasi surat elektronik nya ke lokal berfungsi dengan baik, agar surat elektronik lama dapat diakses dengan mudah;
13. Pengguna harus memberi tanda pada surat elektronik yang berisi data sensitif sebagai rahasia. Proses Transformasi dapat dipergunakan hanya bila dibutuhkan untuk kerahasiaan;
14. Pengguna harus menginformasikan kepada atasannya atau kepada pengelola teknologi jika mereka mengetahui adanya penyalahgunaan sistim surat elektronik;
15. Dilarang mempergunakan surat elektronik untuk hal-hal yang tidak berhubungan dengan pekerjaannya;
16. Dilarang mengirim dan atau mendapatkan materi-materi illegal (kriminal) ataupun mendapatkan materi apapun yang secara eksplisit bersifat seksual, atau yang mempermalukan atau menyerang individu lain atau kelompok tertentu, termasuk dilarang mengirimkan pesan yang memfitnah, melecehkan, mengintimidasi ataupun diskriminatif;
17. Dilarang mengirimkan atau meneruskan surat elektronik berindikasi SPAM secara berantai dalam bentuk apapun;
18. Siapapun dilarang mengakses atau menggunakan surat elektronik milik orang lain tanpa ijin terlebih dahulu dari pemilik alamat surat elektronik orang lain tersebut;
19. Bagi surat elektronik masuk tersimpan yang sudah melebihi kuota, surat elektronik tersebut akan dihapus secara berkala pada saat pemeliharaan sistem bulanan (seminggu sebelum akhir bulan), dan hanya surat elektronik satu minggu terakhir yang tersisa dalam kotak surat elektronik;
20. Pengguna tidak dianjurkan mempergunakan surat elektronik pribadinya untuk dikirimkan ke surat elektronik nama unik BNPB jika tidak terkait dengan pekerjaannya;
21. Semua pesan dan file yang dibuat, dikirim dan diterima dalam sistem surat elektronik menjadi milik BNPB;
22. Pengelola teknologi memberikan batas kuota surat elektronik yang diberlakukan kepada semua pengguna;
23. Pengelola teknologi akan melakukan pengawasan surat elektronik secara berkala secara acak dan cetakan surat elektronik dapat digunakan sebagai bukti dalam pemeriksaan keamanan bila

diperlukan;

24. Pengelola teknologi BNPB memiliki hak untuk mengotorisasi dan mengakses surat elektronik dalam pemeriksaan acak atas fasilitas surat elektronik maupun dalam proses audit;
25. Pengelola teknologi informasi harus memastikan bahwa id pengguna dan kata kunci surat elektronik yang sudah tidak digunakan agar di non aktifkan atau di ulang.

3.9. Cadangan dan Pengembalian File

Tujuan kebijakan ini adalah untuk memberikan sarana bagi pemulihan data dan melanjutkan pekerjaan sesegera mungkin pada saat fasilitas komputer atau jaringan mengalami gangguan yang berdampak besar terhadap proses sistem Informasi.

1. Ruang lingkup kebijakan ini berlaku atas semua informasi file dan data penting milik BNPB dan BPBD yang tersimpan dalam komputer dan penyimpanan data atau perangkat teknologi lainnya termasuk data dan file pada piranti lunak sistem operasi, piranti lunak basis data, piranti lunak aplikasi dan surat elektronik;
2. Semua informasi dan piranti lunak yang bersifat penting, termasuk semua perubahan program dan piranti lunak sistem yang disimpan dalam sistem komputer harus di cadangan secara periodik. Cadangan dilakukan untuk memudahkan pemulihan saat terjadi bencana atau kerusakan system;
3. Jadwal cadangan untuk setiap informasi dan data yang penting harus dibuat, dan seseorang harus ditunjuk secara khusus untuk melakukan cadangan/pengembalian secara teratur;
4. Setiap proses cadangan harus di lakukan sesuai dengan prosedur dan di dokumentasikan dengan baik;
5. Salinan cadangan disimpan secara terpisah di tempat yang aman. Catatan/log dibuat untuk memberikan informasi yang memadai untuk setiap cadangan. Jumlah salinan cadangan yang disimpan dan jangka waktu penyimpanannya harus didasarkan seberapa pentingnya aplikasi dan data yang di cadangan;
6. Salinan cadangan harus diuji secara berkala untuk memastikan data yang disimpan lengkap dan dapat digunakan. Media cadangan yang disimpan di luar kantor harus bisa diambil sewaktu-waktu dan pengambilan data harus dilakukan dengan persetujuan dari pengelola teknologi informasi;
7. Media cadangan harus dilindungi dari kerusakan yang disebabkan perusakan, temperatur yang ekstrim, efek magnetic, dan air. Media dapat berupa tape atau kepingan keras atau disc;
8. Dilarang menyimpan cadangan pada sistem operasi yang terinfeksi virus;
9. Gunakan kata kunci yang aman saat melakukan dan menyimpan

cadangan;

10. Prosedur pengembalian harus diuji secara berkala untuk memastikan integritas dan kelengkapan proses cadangan, juga kegunaan serta kelengkapan salinan cadangan. Permintaan pengembalian beserta alasannya harus dicatat dan didokumentasikan;
11. Pengelola teknologi informasi BNPB harus memiliki minimal dua internet provider (pengelola internet) sebagai strategi cadangan jalur internet. Hal ini berguna untuk cadangan bagi koneksi internet yang terputus dari pengelola internet utama;
12. Semua pengelola teknologi informasi bertanggung jawab untuk melakukan prosedur cadangan dan restorasi yang benar, untuk memastikan tersedianya cadangan yang memadai dan dapat digunakan serta selalu memonitor pelaksanaannya.

3.10. Kontrol Perubahan

Tujuan kebijakan ini adalah untuk memastikan perubahan yang terjadi pada sistem yang berdampak terhadap operasional teknologi informasi BNPB dan BPBD secara keseluruhan diketahui, disetujui dan dikontrol guna mencegah adanya perubahan yang dapat mengancam keamanan dan integritas keseluruhan sistem Informasi. (Formulir ini dapat dilihat pada **lampiran 15 ,16, 17 dan 24**).

1. Ruang lingkup kebijakan ini meliputi semua instalasi sistem baru, implementasi, migrasi sistem, menambal data, relokasi sistem, dan konfigurasi ulang sistem teknologi informasi BNPB dan BPBD;
2. Perubahan pada sistem teknologi informasi yang berdampak pada aktivitas pekerjaan secara keseluruhan harus didokumentasikan dengan baik untuk memudahkan pelacakan dan memastikan referensi yang memadai tersedia yang akan digunakan di masa mendatang. Dokumentasi perubahan meliputi dokumen Kontrol terhadap perubahan, dokumen konfigurasi saat ini, dan dokumen instalasi konfigurasi. Dokumen kontrol perubahan disediakan sebagai dasar persetujuan dan eksekusi perubahan sistem;
3. Pengelola teknologi informasi harus mendokumentasikan semua perubahan seperti perubahan pada sistem operasi, perubahan penyimpanan data dan komponen perangkat lainnya terkait, perubahan aplikasi yang berada di penyimpanan data dan perubahan spesifikasi dan konfigurasi data/komunikasi serta perangkat keamanan;
4. Pengelola teknologi informasi harus menjalankan proses ini di luar jam kerja dan harus memberitahu kepada semua pengguna minimal satu hari sebelumnya;
5. Pengelola teknologi informasi harus memastikan standarisasi konfigurasi sistem operasi untuk mesin-mesin komputer dengan tipe yang sama. Dokumentasi mesin-mesin komputer tersebut harus menggambarkan kesamaannya, agar tersedia referensi yang konsisten.

Referensi yang konsisten menghemat waktu saat terjadi masalah atau saat melakukan trouble shooting pada masalah yang terus menerus terjadi dan khususnya saat dilakukan audit sistem;

6. Pengelola teknologi informasi BNPB dan BPBD bertanggung jawab untuk memastikan proses perubahan sistem yang benar dijalankan untuk menjamin kualitas, keamanan dan integritas sistem serta memonitor pelaksanaannya.

3.11. Dukungan Tenaga Komputer Untuk Pengguna

Tujuan kebijakan ini adalah untuk memberikan pelayanan permasalahan umum pada komputer dan jaringan bagi seluruh pengguna teknologi informasi dan memelihara semua komponen teknologi informasi. Staf yang membantu segala permasalahan teknologi baik di BNPB maupun BPBD adalah staf pengelola teknologi informasi. Permasalahan umum yang ditangani mencakup permasalahan perangkat jaringan, permasalahan perangkat komunikasi (misal radio, perangkat konferensi suara, mobil komunikasi), permasalahan sistem operasi, sistem software, sistem aplikasi, keamanan sistem informasi dan juga perangkat keras lainnya (misal printer, scanner, komputer desktop, notebook, laptop, penyimpanan data, storage media, UPS, switch, router, modem, kabel jaringan). (Formulir ini dapat dilihat pada **lampiran 22**)

1. Ruang lingkup kebijakan ini berlaku bagi seluruh petugas teknologi informasi di BNPB dan BPBD;
2. Secara umum jam operasional adalah jam 08.00 – 17.00, Senin sampai Jum'at. Pada kasus darurat, pengguna dapat menghubungi staf teknologi. Jam operasional akan diberlakukan pelayanan 24 jam setelah terbentuk pusat informasi teknologi informasi;
3. Seluruh petugas teknologi informasi harus mencatatkan semua aktifitas harian yang terjadi dilingkungannya. Hasil pekerjaan yang dilakukan harus mendapat paraf/tanda tangan dari pihak pengguna dan atau wakilnya bila berhalangan. Pihak pengguna adalah seseorang yang meminta bantuan solusi permasalahan teknologi informasi kepada staf teknologi;
4. Pihak pengguna harus memberikan paraf dan informasi pada lembar kerja yang diberikan oleh petugas, setelah pihak petugas selesai menelusuri permasalahan tersebut;
5. Permasalahan yang diketahui sendiri dan ditemukan langsung oleh staf teknologi tetap harus dicatatkan pada laporan harian atau bulanan;
6. Staf teknologi harus segera merespon permintaan penanganan permasalahan dari pihak pengguna dan mencatatkan pada buku laporan permasalahan harian, kemudian menganalisa permasalahan tersebut. Jika hasil analisa tersebut tidak dapat diselesaikan pada hari yang sama maka petugas teknologi informasi harus memberikan catatan tertulis (surat elektronik) mengenai batas waktu penyelesaian

masalah kepada pengguna;

7. Petugas teknologi informasi harus memberikan informasi perkembangan status penanganan masalah yang masih tertunda kepada pengguna setiap harinya, hal ini dilakukan jika masalah tersebut masih belum selesai pada hari kerja berikutnya;
8. Petugas teknologi informasi harus meminta bantuan kepada staf teknologi informasi yang lebih senior terhadap permasalahan yang tidak dapat ditangani dan atau membutuhkan level akses lebih tinggi;
9. Pembagian tugas kerja di dalam pelayanan permasalahan teknologi informasi minimal harus terdiri dari;
10. Satu staf system administrator yang bertugas melayanani permasalahan untuk akses level yang lebih tinggi baik masalah jaringan, masalah keamanan sistem operasi dan sistem aplikasi serta perangkat keras pada ruang penyimpanan data (area terbatas);
11. Dua staf tenaga informasi teknologi yang bertugas melayani permasalahan umum komputer dan jaringan dan sistem aplikasi serta perangkat keras, dan perangkat komunikasi. Akses level petugas ini di bawah system administrator;
12. Petugas teknologi informasi harus membuat laporan harian dan dikirimkan kepada atasan terkait;
13. BNPB dan BPBD bertanggung jawab untuk memastikan tersedianya staf untuk tenaga pengelola teknologi informasi yang baik dan berkualitas;
14. Seluruh karyawan BNPB dan BPBD dan juga kepada pihak ketiga yang terikat kerjasama dengan BNPB atau BPBD harus mematuhi kebijakan ini.

3.12. Penanganan Masalah Teknologi Informasi

Tujuan kebijakan ini adalah untuk memastikan bahwa masalah yang terjadi di lingkungan teknologi informasi dapat ditangani, diselesaikan dan dilaporkan dalam rangka mempertahankan kelangsungan operasional kerja di BNPB dan BPBD. (Formulir ini dapat dilihat pada **lampiran 23**).

1. Ruang lingkup kebijakan ini berlaku untuk semua insiden dan masalah di bidang teknologi informasi yang tidak dikategorikan sebagai dan yang berpotensi mempengaruhi operasional kerja BNPB dan BPBD;
2. Setiap peristiwa yang bukan merupakan bagian dari operasi standar, seperti sebuah masalah dan kesalahan yang terjadi di bidang teknologi informasi harus langsung segera dilaporkan;
3. Pengelola teknologi informasi di BNPB dan BPBD harus memadai dalam menangani dan memecahkan masalah di areanya serta melakukan identifikasi masalah untuk memastikan bahwa masalah ini diselesaikan secara efisien pada waktu yang tepat;

4. Eskalasi permasalahan pada setiap kategori masalah harus dijalankan ketika masalah tidak dapat diselesaikan dalam tingkat yang lebih rendah;
5. Solusi untuk permasalahan yang mengganggu seluruh operasional kerja harus dikonsultasikan ke dan dikoordinasikan dengan pengelola teknologi informasi yang lebih senior;
6. Fasilitas sistem audit trail harus disediakan terlebih dahulu di semua bagian yang relevan. Hal ini memungkinkan penelusuran pelacakan masalah dan penyebab yang ditimbulkan;
7. Sebuah masalah yang tepat dan laporan kejadian harus dibentuk untuk merekam masalah yang terjadi. Dokumentasi tersebut harus dipelihara guna mencegah dan mengatasi insiden yang serupa terjadi;
8. Seluruh pengelola teknologi informasi bertanggung jawab untuk memastikan insiden dan masalah yang dikelola dengan baik dan diselesaikan secara tepat waktu;
9. Seluruh pengelola teknologi informasi di BNPB dan BPBD harus mematuhi kebijakan ini.

3.13. Manajemen Servis Level

Tujuan kebijakan ini adalah untuk mendefinisikan pengelolaan tingkat layanan antara penyedia jasa dan pengguna jasa mengenai mutu layanan dari keseluruhan strategi teknologi informasi dalam lingkungan BNPB dan BPBD, dalam rangka mempertahankan performa kerja yang dapat diterima untuk mendukung operasional kerja BNPB dan BPBD secara keseluruhan. Manajemen Servis Level (Service Level Management) bukanlah sebuah kontrak kerja, namun lebih merupakan kesepakatan tentang mutu layanan servis.

1. Ruang lingkup kebijakan ini berlaku untuk layanan perjanjian antara pengelola teknologi informasi di BNPB dan BPBD serta seluruh pengguna;
2. Sebuah perjanjian tingkat layanan formal harus secara eksplisit menentukan tingkat layanan yang diberikan (misalnya ketersediaan layanan, keandalan, kinerja, kapasitas untuk pertumbuhan, tingkat dukungan yang diberikan kepada pengguna), secara kuantitatif dan kualitatif;
3. Layanan pengguna harus membatasi tuntutan atas layanan dalam batas-batas yang disepakati;
4. Ragam dan tanggung jawab untuk kinerja yang mengatur hubungan antara semua pihak yang terlibat harus jelas ditetapkan, dikoordinasikan, dikelola dan dikomunikasikan kepada semua pihak yang terkena dampak;
5. Kinerja pelayanan harus dipantau secara tepat waktu berdasarkan tingkat setuju dan prestasi serta masalah yang harus dilaporkan;
6. Tanggung jawab pengelolaan servis level ini pada semua pengelola teknologi di BNPB dan BPBD guna memastikan tersedia pelayanan

yang tertuang dalam kesepakatan, kinerja. Tindakan perbaikan yang dilakukan untuk mengembalikan layanan ketingkat yang telah disepakati;

7. Seluruh pengelola teknologi informasi di BNPB dan BPBD harus mematuhi kebijakan ini.

3.14. Pengadaan Sistem dan Perangkat Teknologi Informasi

Tujuan kebijakan ini adalah memberikan metode standar dalam prosedur pengadaan sistem dan perangkat teknologi informasi dan dapat memberikan solusi dengan cara yang hemat serta menjaminkan kualitas yang sesuai bagi teknologi informasi BNPB dan BPBD.

1. Ruang lingkup kebijakan ini berlaku untuk semua kebutuhan akan sistem dan perangkat teknologi informasi yang dilakukan oleh pengelola teknologi informasi di BNPB dan BPBD;
2. Tahapan untuk pengadaan sistem dan perangkat teknologi informasi harus mendapat masukan dan partisipasi dari unit-unit pengguna yang terkait dalam hal tersebut;
3. Rencana dasar pengadaan harus sesuai dan cukup untuk dilakukan kontrol atas proyek guna memantau waktu dan biaya yang dikeluarkan selama pengadaan berlangsung;
4. Setiap implementasi pengadaan harus ditulis dan definisikan dengan jelas sesuai sifat pengadaan dan ruang lingkupnya sebelum pekerjaan pengadaan dimulai;
5. Setiap pengadaan yang diusulkan harus menjalani studi kelayakan yang lengkap, dan laporan harus ditinjau oleh pimpinan teknologi informasi sebagai dasar bagi keputusan tentang keberlangsungan/kelanjutan dari pengadaan;
6. Pekerjaan pengadaan harus diselesaikan dalam setiap tahap dan sebelum bekerja harus mendapat persetujuan dari unit-unit terkait atau pihak yang terkait dengan pengadaan pada fase berikutnya dimulai;
7. Sebuah pengadaan menerapkan sistem baru atau diubah harus mencakup penyusunan rencana mutu, yang secara resmi dikaji dan disepakati oleh semua pihak yang terkait dengan pengadaan tersebut;
8. Analisa risiko formal harus dilaksanakan untuk menghilangkan atau meminimalkan risiko;
9. Peninjauan ulang pelaksanaan pengadaan harus dimasukkan sebagai bagian integral dari setiap rencana pengadaan, untuk memastikan apakah pengadaan tersebut bermanfaat sesuai yang direncanakan;
10. Pimpinan pengelola teknologi informasi BNPB dan BPBD bertanggung jawab dalam mengembangkan rencana pengadaan teknologi informasi yang sesuai dengan rencana strategi teknologi informasi BNPB;
11. Seluruh karyawan BNPB dan BPBD dan atau pihak ketiga yang terkait pengadaan harus mematuhi kebijakan ini.

BAB IV

KEBIJAKAN PENGELOLAAN KOMPONEN TEKNOLOGI INFORMASI

Kebijakan pengelolaan komponen teknologi informasi di BNPB dan BPBD dapat diklasifikasikan dalam lima kebijakan yang dijelaskan sebagai berikut.

1. Kebijakan Standar Lingkungan Operasi
2. Kebijakan Uji Kelayakan dan Serah Terima
3. Kebijakan Inventori Perangkat Teknologi
4. Kebijakan Hibah Komponen Teknologi Informasi BNPB Kepada BPBD
5. Kebijakan Laporan Kehilangan Komponen Teknologi

4.1. Standar Lingkungan Operasi

Tujuan kebijakan ini adalah untuk menyediakan standar komponen teknologi informasi agar memudahkan pengendalian dan menjamin integrasi sistem yang terkontrol dalam pengelolaannya. Standar Lingkungan Operasi (SLO) adalah standarisasi terhadap penggunaan semua komponen teknologi informasi di BNPB dan BPBD. (Formulir SLO dapat dilihat pada **lampiran 1,2,3,4,5 dan 6**).

1. Ruang lingkup kebijakan ini berlaku untuk semua komponen teknologi yang digunakan di BNPB dan BPBD;
2. Standar Lingkungan Operasi ini harus didefinisikan dalam daftar SLO dan diperbaharui pada tahun berikutnya sesuai dengan perkembangan teknologi terkini;
3. Platform yang ditetapkan untuk perangkat lunak sistem operasi utama pada sistem informasi di BNPB dan BPBD adalah sistem operasi berbasis Windows. Secara bertahap platform perangkat lunak akan menggunakan sistem terbuka. Sistem operasi lainnya tidak menjadi standar sistem operasi BNPB dan BPBD;
4. Perangkat lunak yang digunakan adalah versi yang dikeluarkan perangkat lunak tersebut pada lima tahun terakhir;
5. Pertimbangan rasional akan diberikan kepada pengguna untuk perangkat lunak lain yang sesuai dengan daftar SLO dalam mendukung pekerjaannya;
6. Tanggung jawab atas pengujian semua perangkat teknologi dan legalitas lisensi perangkat lunak dipegang oleh pengelola teknologi informasi BNPB. Pengelola teknologi informasi di BPBD dapat mengelola lisensi perangkat lunak di wilayah/daerahnya dengan tetap merujuk pada kebijakan ini;
7. Seluruh karyawan dan atau pihak ketiga yang berkepentingan dengan BNPB dan BPBD yang mengoperasikan fasilitas teknologi harus mematuhi kebijakan ini.

4.2. Uji Kelayakan dan Serah Terima

Tujuan kebijakan ini adalah untuk memberikan prosedur standar untuk menentukan kesesuaian kebutuhan teknologi informasi yang diminta dan harus sesuai dengan rencana strategi BNPB.

1. Ruang lingkup uji kelayakan dan serah terima berlaku terhadap pengadaan barang perangkat keras dan perangkat lunak teknologi informasi;
2. Pengelola teknologi informasi harus bekerja sama dengan panitia penerima barang dan jasa yang akan menerima komponen serta mempersiapkan prosedur uji kelayakan tersebut;
3. Uji kelayakan harus menjelaskan rencana pemasangan dan penggunaan komponen yang akan diakuisisi;
4. Uji kelayakan dilakukan oleh pengguna teknologi di BNPB dan BPBD dengan menjelaskan spesifikasi perangkat lunak atau perangkat keras, persyaratan pemrosesan, biaya tahunan dari pengoperasian perangkat berikut daftar hasil atau peningkatan yang diharapkan setelah perangkat atau sistem dipasang serta level staf yang dibutuhkan;
5. Dokumen lisensi dan petunjuk penggunaan harus ada untuk setiap perangkat lunak dan perangkat keras serta dicatat dalam catatan persediaan (inventori);
6. Uji kelayakan harus diselesaikan dan disetujui sebelum komponen teknologi informasi tersebut diakuisisi dan diserah terimakan;
7. Uji kelayakan digunakan sebagai dasar bagi BNPB dan BPBD untuk memutuskan apakah perangkat lunak atau perangkat keras baru yang diajukan dapat diterima;
8. Pengelola teknologi informasi BNPB dan BPBD harus memastikan uji kelayakan dilakukan dengan benar sebelum dilakukan serah terima perangkat atau sistem yang baru. Pengelola teknologi bertanggung jawab dalam pelaksanaan dan mematuhi kebijakan ini;

4.3. Inventori Perangkat Teknologi

Tujuan kebijakan ini adalah untuk memastikan bahwa inventori peralatan teknologi informasi telah dikelola dan diatur dengan baik dalam penggunaannya serta memastikan memiliki dokumentasi yang cukup untuk kebutuhan BNPB dan BPBD. (Formulir ini dapat dilihat pada **lampiran 21**).

1. Ruang lingkup inventori meliputi komponen perangkat keras dan perangkat lunak teknologi informasi yang terdaftar di BNPB dan BPBD;
2. Semua perangkat/komponen teknologi yang berada dalam tanggung jawab pengelola teknologi informasi harus diinventarisir dan disimpan pada ruang terpisah atau ruang inventori serta harus dikelola jumlah stok dan statusnya dalam dokumen inventori;

3. Hanya pengelola teknologi yang mendapat izin boleh memasuki ruang inventori. Selain staf teknologi harus mendapat ijin dari pimpinan pengelola teknologi dan melengkapi buku catatan untuk masuk ke dalam area terbatas ruang inventori;
4. Hanya pengelola teknologi yang memiliki otorisasi untuk melakukan perbaikan dan menggunakan perlengkapan yang disimpan di dalam ruang inventori;
5. Penggunaan perlengkapan dan suku cadang perangkat teknologi hanya untuk kepentingan operasional kerja BNPB dan BPBD. Penggunaan peralatan dan suku cadang harus disertai dokumen resmi yang menerangkan tujuan penggunaannya dan harus diketahui oleh staf pengelola teknologi Informasi;
6. Inventori peralatan teknologi harus dikelola di bawah pengawasan pengelola teknologi informasi. Catatan untuk setiap tipe barang harus dibuat termasuk catatan pengiriman, distribusi, penggunaan serta pembuangan barang;
7. Pemeriksaan rutin atas inventori dilakukan oleh petugas Barang Milik Negara dibawah pengawasan pengelola teknologi guna memastikan penggunaannya;
8. Pengelola teknologi bertanggung jawab untuk memastikan inventori perangkat teknologi yang dimiliki telah dipergunakan dengan benar sesuai standar keamanan akses ruang terbatas;
9. Tanggung jawab kebijakan ini dipegang oleh pengelola teknologi BNPB dan BPBD yang sudah memilki prosedur penyimpanan inventori.
10. Seluruh pengelola teknologi informasi BNPB dan BPBD harus mematuhi kebijakan ini.

4.4. Hibah Komponen Teknologi Informasi BNPB Kepada BPBD

Tujuan kebijakan ini adalah untuk memastikan prosedur pemberian hibah perangkat teknologi informasi baik perangkat keras ataupun perangkat lunak yang dihibahkan oleh BNPB kepada BPBD dapat teralokasi dan terdokumentasi dengan benar sesuai kebutuhan dan pemanfaatannya oleh BPBD. (Formulir ini dapat dilihat pada **lampiran 18, 19 dan 20**)

1. Ruang lingkup kebijakan hibah komponen teknologi dari BNPB kepada BPBD meliputi:
   a. Perangkat keras, perangkat lunak dan perangkat jaringan.
   b. Peralatan Global Positioning System (GPS) dan perangkat pendukungnya.
   c. Perangkat Radio Komunikasi dan perangkat pendukungnya.
   d. Komunikasi Mobil dan perangkat pendukungnya.
   e. Perangkat teknologi lainnya.
2. BPBD wajib menggunakan komponen hibah dalam mendukung operasional penanggulangan kebencanaan dengan optimal;

3. Semua item perangkat yang dihibahkan harus tercatat lengkap dan dibuatkan laporan secara terpisah oleh BNPB;
4. Setiap tiga bulan BPBD penerima hibah komponen teknologi informasi wajib membuat laporan evaluasi penggunaan dan kondisi komponen serta membuat rekomendasi terhadap permasalahan yang ada;
5. Efektifitas penggunaan hibah peralatan di BPBD menjadi dasar dalam penentuan hibah selanjutnya;
6. Seluruh pihak baik unit atau deputi yang akan menghibahkan perangkat/peralatan teknologi harus bekerjasama dengan pengelola teknologi informasi BNPB.

4.5. Laporan Kehilangan Komponen Teknologi

Tujuan kebijakan ini adalah untuk memberikan petunjuk kepada semua pengguna dalam melaporkan kehilangan atau pencurian komponen teknologi informasi. (Formulir ini dapat dilihat pada **lampiran 13** dan **14**).

1. Ruang lingkup kebijakan ini berlaku untuk semua komponen teknologi informasi di BNPB dan BPBD;
2. Setiap staf harus menjaga perangkat teknologi informasi dilingkungannya dari kerusakan dan pencurian;
3. Seluruh staf bertanggung jawab untuk melaporkan semua kejadian kehilangan pada kantor polisi terdekat dan kepada staf pengelola teknologi informasi;
4. Seluruh staf wajib mengisi buku catatan barang hilang, apabila terjadi kehilangan komponen teknologi dengan melampirkan surat kehilangan dari kantor polisi terdekat;
5. Seluruh staf yang mengoperasikan fasilitas teknologi informasi bertanggung jawab untuk memastikan keamanan perangkatnya dan menyadari resiko keamanan atas perangkat tersebut;
6. Kepala Pelaksana pengelola teknologi informasi di setiap wilayah / area kerjanya masing-masing bertanggung jawab untuk melakukan pemeriksaan rutin dan memastikan ketaatan atas kebijakan ini.

BAB V
KEBIJAKAN PENGELOLAAN APLIKASI SISTEM INFORMASI

Aplikasi sistem informasi adalah program komputer yang dibuat untuk mendukung operasional kerja BNPB dan BPBD. Aplikasi sistem informasi yang dimiliki dan dikembangkan oleh BNPB terbagi menjadi dua, yaitu aplikasi sistem informasi kebencanaan dan aplikasi sistem informasi non kebencanaan.

a. Aplikasi sistem informasi kebencanaan mengelola data kebencanaan di Indonesia dari mulai pra bencana, pada saat bencana dan pasca bencana. Aplikasi sistem informasi kebencanaan yang berlaku di BNPB dan BPBD adalah Sistem Informasi Kebencanaan Terpadu. Aplikasi ini bertujuan untuk menggabungkan dan mensinkronisasikan fungsi dari aplikasi-aplikasi kebencanaan sebelumnya yang sudah digunakan menjadi aplikasi yang terpadu. Aplikasi SINDU merupakan sistem penunjang keputusan untuk mendukung operasional penanggulangan kebencanaan dan menjadi salah satu dasar dalam proses pemberian dana on call. Aplikasi SINDU akan dikembangkan menjadi satu-satunya aplikasi kebencanaan yang digunakan oleh BNPB dan BPBD;
b. Aplikasi sistem informasi non kebencanaan adalah aplikasi yang mengolah data selain data kebencanaan. Aplikasi non kebencanaan lebih pada aplikasi administratif, misalnya aplikasi kepegawaian, aplikasi persuratan, aplikasi inventaris. Aplikasi ini menggunakan teknologi aplikasi lokal atau aplikasi pada jaringan kerja lokal.

Tujuan dari kebijakan ini adalah untuk memastikan bahwa sistem aplikasi yang akan diimplementasikan dan dikembangkan harus sesuai dengan metodologi yang berlaku dan sejalan dengan strategi dan rencana jangka panjang BNPB. Kebijakan pengelolaan sistem aplikasi teknologi informasi BNPB dapat diklasifikasikan dalam tujuh kebijakan yang dijelaskan sebagai berikut.

1. Kebijakan Penggunaan Aplikasi Sistem Informasi;
2. Kebijakan Standarisasi Teknis Aplikasi Sistem Informasi;
3. Kebijakan Implementasi Aplikasi Sistem Informasi;
4. Kebijakan Dokumentasi dan Petunjuk Teknis Aplikasi Sistem Informasi;
5. Kebijakan Pengelolaan Nama unik dan Intranet;
6. Kebijakan Pengelolaan File dan Data Aplikasi;
7. Kebijakan Bimbingan Teknis Aplikasi Sistem Informasi

5.1. Penggunaan Aplikasi Sistem Informasi

Tujuan kebijakan ini adalah agar implementasi dan pengembangan aplikasi sistem informasi di BNPB dan BPBD menjadi lebih terpadu dan tidak tumpang tindih, sehingga pengelolaan dan penggunaannya dapat lebih optimal dan lebih efisien. Strategi pengembangan aplikasi sistem informasi adalah sebagai berikut.

1. Ruang lingkup kebijakan ini mencakup implementasi, modifikasi dan pengembangan sistem aplikasi di BNPB dan BPBD;
2. Pengembangan dan implementasi aplikasi sistem informasi di BNPB harus dapat saling terintegrasi dengan cara menerapkan sistem operasi dan sistem basis data yang sama dan standar;
3. Implementasi dan pengembangan aplikasi harus menuju kepada konsep sistem basis data satu pintu, sehingga mempermudah penggunaan oleh BPBD dan mempermudah pengelolaan dan pengembangan lebih lanjut;
4. Sesuai dengan PERKA BNPB No 1 tahun 2008 tentang Organisasi dan Tata Kerja BNPB, Pusdatinmas BNPB bertanggung jawab untuk melaksanakan pengkoordinasian terhadap pengelolaan sistem aplikasi kebencanaan di BNPB. Secara bertahap, seluruh sistem aplikasi kebencanaan yang ada di BNPB akan diintegrasikan atau disinkronisasikan ke dalam aplikasi SINDU;
5. Seluruh pengguna sistem Informasi kebencanaan di BNPB dan BPBD wajib menggunakan aplikasi yang sudah diintegrasikan ke dalam SINDU dalam mendukung pekerjaannya;
6. Unit-unit di dalam BNPB dan BPBD adalah pemilik dan penanggung jawab kualitas dan kuantitas data dan informasi serta pembuatan laporan sesuai dengan tugas dan fungsinya masing-masing;
7. Hanya operator data di unit terkait di BNPB atau operator data di BPBD yang dapat melakukan masukan data pada aplikasi. Operator data harus memasukkan informasi yang benar dan dapat dipertanggungjawabkan. Petugas selain operator yang melakukan masukan/merubah data harus mendapat ijin dari atasan terkait di unit terkait atau atasan di BPBD;
8. Bagian pengelola teknologi dan unit-unit pemilik aplikasi secara berkala melakukan evaluasi terhadap aplikasi untuk mendapatkan kualitas dan kuantitas data yang lebih lengkap dan akurat serta melakukan perbaikan dan pengembangan-pengembangan yang dianggap perlu;
9. Pengelola teknologi informasi di Pusdatinmas BNPB bertanggung jawab mengimplementasikan dan menyempurnakan aplikasi SINDU agar sesuai dengan kebutuhan di BNPB dan BPBD;
10. Seluruh pengelola teknologi informasi berfungsi sebagai pemberi dukungan teknis terhadap penggunaan infrastruktur teknologi informasi yang digunakan oleh sistem aplikasi;
11. Seluruh pengelola teknologi informasi bertanggung jawab untuk memastikan proses akuisisi dan implementasi dijalankan dengan benar serta harus menjamin kualitas dan kesesuaian sistem dengan tuntutan kepentingan dan tujuan jangka panjang teknologi informasi BNPB.

5.2. Standarisasi Teknis Aplikasi Sistem Informasi

Tujuan kebijakan ini adalah untuk memastikan aplikasi yang akan digunakan di BNPB dan BPBD memiliki spesifikasi teknis yang sama, sehingga dapat mempermudah untuk melakukan sinkronisasi antar aplikasi dan memudahkan pengembangan ke depan. Standarisasi teknis aplikasi adalah sebagai berikut.

1. Ruang lingkup kebijakan ini meliputi semua pengguna aplikasi kebencanaan dilingkungan BNPB dan BPBD;
2. Aplikasi harus dapat menerima format basis data yang berbeda untuk disinkronisasi ke dalam basis data terpadu;
3. Sistem basis data menggunakan teknologi yang dapat mengelola data dalam kapasitas besar;
4. Sistem operasi dianjurkan bersifat terbuka, kebijakan ini akan dibakukan saat BNPB menetapkan perubahan infrastruktur secara menyeluruh;
5. Aplikasi harus dapat mudah dikembangkan menjadi aplikasi berbasis web internet dan atau Intranet;
6. Aplikasi harus memiliki minimal fungsi-fungsi sebagai berikut;
   a. Fungsi pelacakan data untuk kebutuhan audit dan keamanan;
   b. Fungsi keamanan, seperti peraturan kata kunci, keamanan dari tindakan pencurian data ;
   c. Fungsi cadangan-pengembalian yang lengkap. Mudah di cadangan dan pengembalian sesuai keperluan;
   d. Basis data harus mampu dilakukan migrasi;
   e. Memilki kemudahan instalasi baik di dalam penyimpanan data atau komputer pengguna;
   f. Mampu dilakukan pengujian pada tes untuk proses Tes Penerimaan Pengguna;
   g. Harus memiliki akun id pengguna dan Kata kunci pada aplikasi yang diakses bersama;
7. Aplikasi harus memiliki kelengkapan dokumentasi teknis dan petunjuk penggunaan yang lengkap;
8. Seluruh pengguna aplikasi kebencanaan BNPB dan BPBD wajib mematuhi kebijakan ini;
9. Seluruh pengelola teknologi bertanggung jawab terhadap kepatuhan atas kebijakan ini.

5.3. Implementasi Aplikasi Sistem Informasi

Tujuan kebijakan ini adalah untuk memastikan prosedur implementasi aplikasi sistem baru harus sejalan dengan rencana kerja jangka panjang di BNPB dan harus sesuai dengan metodologi/tahapan sebagai berikut.

1. Ruang lingkup kebijakan ini meliputi semua pengguna yang akan

melakukan pengembangan sistem aplikasi baru dilingkungan BNPB dan BPBD;

2. Dalam membuat perencanaan aplikasi sistem informasi, unit-unit terkait harus melibatkan pengelola teknologi informasi agar aplikasi yang akan dibangun dapat terintegrasi dan tidak tumpang tindih;
3. Khusus untuk aplikasi-aplikasi sistem informasi kebencanaan, maka basis data harus menggunakan spesifikasi sistem basis data yang sama dengan sistem yang sudah ada (untuk kemudahan migrasi atau pengembangan aplikasi dimasa mendatang) jika harus mengalami perbedaan spesifikasi sistem basis data maka harus dibuatkan aplikasi pendukung untuk mempermudah proses masukan dan keluaran bagi aplikasi berbeda.
4. Kontrol pembuatan aplikasi dilakukan secara rutin oleh unit-unit pemilik aplikasi bersama dengan pengelola teknologi informasi terhadap pengembang aplikasi sistem informasi;
5. Migrasi data dari aplikasi lama ke aplikasi baru dilakukan oleh pengelola teknologi informasi dengan dukungan dari pengembang aplikasi termasuk pihak ketiga, misalnya vendor atau konsultan (Formulir ini dapat dilihat pada **lampiran 24**);
6. Pengembang aplikasi bersama dengan pengelola teknologi informasi dan unit pemilik aplikasi berkewajiban memberikan pelatihan lengkap dan jelas kepada seluruh pengguna aplikasi sebelum melakukan serah terima. Pengguna aplikasi harus mendapatkan buku petunjuk pemakaian aplikasi yang lengkap;
7. Serah terima aplikasi sistem informasi harus mengikuti prosedur uji kelayakan dan serah terima yang ditentukan, dan harus dilengkapi dokumen teknis aplikasi yang lengkap yang telah disetujui oleh pengelola teknologi informasi;
8. Uji coba dilakukan minimal selama tiga bulan setelah pelatihan, permasalahan yang timbul selama masa uji coba menjadi tanggung jawab pengembang aplikasi untuk melakukan perbaikan;
9. Implementasi dilakukan setelah masa uji coba aplikasi selesai dengan lengkap dan baik. Pada saat implementasi, akses ke aplikasi lama harus ditutup dan aplikasi baru resmi mulai digunakan;
10. Penggunaan aplikasi hanya dapat diakses oleh pengguna yang sudah ditentukan oleh pengelola teknologi informasi. Staf administrasi sistem harus memastikan untuk menutup jalur komunikasi data bagi pihak-pihak yang tidak mendapat hak akses ke aplikasi;
11. Evaluasi aplikasi harus dilakukan terhadap kualitas dan kuantitas data, serta berdasarkan perkembangan kebutuhan dan perkembangan teknologi yang ada.

5.4. Dokumentasi dan Petunjuk Teknis Aplikasi Sistem Informasi

Tujuan kebijakan ini adalah agar semua aplikasi sistem informasi harus memiliki kelengkapan dokumentasi. Dokumentasi aplikasi adalah penjabaran tertulis atas spesifikasi teknis dari aplikasi sistem termasuk petunjuk teknis penggunaan aplikasi. Dokumentasi sistem aplikasi harus berisi:

1. Ruang lingkup kebijakan ini meliputi seluruh dokumen aplikasi, dokumen informasi infrastruktur di BNPB dan BPBD.
2. Struktur data, Kamus data dan perintah pengoperasian yang dibuat oleh pengembang aplikasi.
3. Deskripsi dan format untuk laporan yang dicetak, tampilan layar, dan file-file yang digunakan dalam aplikasi.
4. Deskripsi setiap modul untuk setiap forulir harus ditulis terperinci, baik masuk, proses dan keluar.
5. Deskripsi perangkat keras yang dibutuhkan, deskiripsi konfigurasi, deskiripsi sistem operasi, termasuk deskiripsi perangkat lunak basis data, dan perangkat lunak jaringan yang dibutuhkan untuk mengoperasikan aplikasi sistem informasi.
6. Dokumentasi lengkap petunjuk manual dan penanganan permasalahan.
7. Dokumentasi manual dan tampilan layar pada setiap modul aplikasi harus sesuai.
8. Dokumentasi aplikasi sistem informasi harus memiliki nomor indeks setiap versi aplikasi.
9. Dokumentasi tentang cara instalasi dan penghapusan aplikasi termasuk dokumentasi cara cadangan data dan pengembalian data dan aplikasi pada perangkat penyimpanan data dan atau komputer.
10. Dokumentasi harus disimpan pada tempat yang teratur dan aman oleh pengelola teknologi informasi.
11. Petunjuk Teknis penggunaan aplikasi dibuat dalam dokumen terpisah dan diberi penomoran sesuai dengan perubahan versi aplikasinya.
12. Bagian teknologi informasi bertanggung jawab untuk memastikan tersedianya dokumentasi sistem yang memadai untuk tiap sistem yang dikembangkan di BNPB dan BPBD.

5.5. Pengelolaan Nama unik dan Internet

Tujuan kebijakan ini adalah sentralisasi grup jaringan komputer yang memiliki tingkat keamanan dan control Protokol Internet yang lebih baik. Sistem aplikasi berbasis intranet digunakan untuk dapat diakses oleh pengguna baik BNPB dan BPBD. Pemberian standarisasi nama unik bertujuan untuk memastikan bahwa aplikasi intranet yang digunakan adalah aplikasi resmi BNPB dan BPBD dan berguna menghindari potensi kesalahan informasi yang akan digunakan oleh pihak lain.

1. Ruang lingkup kebijakan ini meliputi semua penggunaan nama unik dan intranet dilingkungan BNPB dan BPBD;
2. Seluruh penamaan aplikasi berbasis internet BNPB dan BPBD harus menggunakan nama unik **go.id;**
3. Alamat situs web resmi BNPB adalah: **www.bnpb.go.id;**
4. Penamaan alamat website untuk BPBD dengan dua cara:
   a. Mengikuti penamaan nama unik (menjadi sub nama unik) situs web Pemda, yaitu: **bpbd.namapemda** contohnya: **bpbd.slemankab**
   b. Penamaan mandiri, yaitu penamaan untuk BPBD yang Pemdanya belum memiliki alamat nama unik internet resmi. Aturan penamaannya adalah sebagai berikut : **bpbd-namakabupaten.go.id** contohnya: **bpbd-yapen.go.id**
5. Penamaan alamat untuk aplikasi web dan intranet adalah: **namaaplikasi.bnpb.go.id** contohnya: **sindu.bnpb.go.id**;
6. BNPB dan BPBD tidak diperbolehkan menggunakan nama diluar pedoman penamaan di atas sebagai situs web resmi;
7. Perubahan atau penambahan nama nama unik harus melalui persetujuan pimpinan Pusdatinmas BNPB;
8. Seluruh pihak yang membutuhkan penggunaan nama unik dan intranet wajib mematuhi kebijakan ini.

5.6. Pengelolaan File dan Data Aplikasi

Merujuk pada Peraturan Kepala BNPB Nomor 8 Tahun 2010 tentang Standardisasi Data Kebencanaan yang bertujuan sebagai berikut.

1. Menyamakan persepsi antara BNPB dan BPBD, Kementerian/Lembaga terkait dan pemangku kepentingan lainnya yang melakukan pengelolaan data bencana;
2. Memberikan panduan dalam pengelolaan data bencana;
3. Mempermudah BNPB dan BPBD, Kementerian/Lembaga Terkait dan pemangku kepentingan lainya dalam pengumpulan, pemrosesan, analisis dan pelaporan data bencana, pada saat pra bencana, tanggap darurat maupun rehabilitasi dan rekonstruksi.

Tujuan kebijakan ini adalah untuk menetapkan standar penggunaan sistem file dan data aplikasi dalam meningkatkan keamanan data, kemudahan akses, serta penanganan file dan data di seluruh aplikasi sistem informasi BNPB dan BPBD yang diatur sebagai berikut.

1. Ruang lingkup kebijakan ini meliputi seluruh file dan data aplikasi untuk sistem informasi di BNPB dan BPBD;
2. Penempatan file aplikasi harus berada di pusat data dan dikelola oleh pengelola teknologi informasi;

3. File aplikasi harus dipisahkan dari kelompok file umum dan harus di cadangan secara berkala;
4. File aplikasi harus di simpan dalam indeks sesuai dengan versinya agar mudah dalam pengelolaan file. Penomoran versi harus diberikan pada setiap perubahan aplikasi;
5. Penyimpanan file aplikasi pada versi sebelumnya harus disimpan di tempat terpisah dan harus dipastikan akses keamanannya;
6. File dan data yang tersimpan dalam penyimpanan data dan atau di komputer adalah data milik BNPB atau BPBD;
7. Segala hal tentang pengelolaan data, file dan dokumentasi terkait sistem informasi dan keamanan menjadi tugas dan tanggung jawab bagian pengelola teknologi informasi;
8. Semua pengguna file dan data wajib mematuhi kebijakan ini dan menyadari resiko keamanan atas hal ini.

5.7. Bimbingan Teknis Aplikasi Sistem Informasi

Tujuan kebijakan ini adalah untuk memberikan panduan lengkap penggunaan sistem aplikasi melalui bimbingan teknis agar pengguna dapat menggunakan aplikasi dengan tepat dan benar. (Formulir ini dapat dilihat pada **lampiran 25**).

1. Ruang lingkup kebijakan ini berlaku untuk semua pelaksanaan implementasi aplikasi baru dan permintaan bimbingan teknis khusus dari internal di BNPB dan BPBD;
2. Pengguna aplikasi wajib mendapat bimbingan teknis atau pelatihan sebelum suatu aplikasi baru diimplementasikan. Unit-unit pemilik aplikasi baru tersebut bersama pengembang aplikasi bertanggung jawab atas pelaksanaaan dan penyediaan materi;
3. Materi bimbingan teknis berisi dokumentasi dan instruksi yang jelas bagi pengguna. Materi tersebut harus menjelaskan konteks secara menyeluruh terhadap sistem yang ada dan menjelaskan juga tentang kemampuan aplikasi baru tersebut dapat mendukung operasional BNPB dan BPBD;
4. Bimbingan teknis harus mencakup praktek menggunakan aplikasi baru, dan harus dipastikan bahwa pengguna memperoleh pengetahuan dan kemampuan yang cukup untuk mengoperasikan aplikasi tersebut terkait dengan pekerjaan mereka masing-masing;
5. Untuk aplikasi informasi kebencanaan, setiap peserta harus juga memberikan bimbingan teknis yang sama kepada minimal tiga orang pengguna aplikasi di daerahnya masing-masing;
6. BPBD dapat melakukan permintaan bimbingan teknis penggunaan aplikasi di tempat kerja kepada BNPB;
7. Pengelola teknologi informasi dan unit-unit pemilik aplikasi harus menyediakan dukungan pasca bimbingan teknis yang terkait dengan penggunaaan aplikasi kepada pengguna;

8. Pengelola teknologi informasi dan unit-unit pemilik aplikasi bertanggung jawab memastikan tersedianya bimbingan teknis yang memadai bagi pengguna aplikasi.

BAB VI
KEBIJAKAN KEAMANAN TEKNOLOGI INFORMASI

Kebijakan keamanan teknologi informasi BNPB dapat diklasifikasikan dalam sembilan kebijakan yang dijelaskan sebagai berikut.

1. Kebijakan Penggunaan Komputer
2. Kebijakan Pengamanan Area Terbatas
3. Kebijakan Akun Pengguna
4. Kebijakan Perlindungan Terhadap Virus
5. Kebijakan Kata kunci
6. Kebijakan Penggunaan Informasi Dan Data
7. Kebijakan Pengendali Jarak Jauh dan Jaringan Tanpa Kabel
8. Kebijakan Operasional Informasi Teknologi Dalam Keadaan Darurat
9. Kebijakan Perlindungan Sistem Informasi Teknologi

6.1. Penggunaan Komputer

Tujuan kebijakan ini adalah memastikan bahwa seluruh komponen teknologi informasi properti milik BNPB atau BPBD dapat terhindar dari penyalahgunaan oleh pihak yang tidak berhak, dan melindungi dari kerusakan fisik dan internalnya serta memastikan penggunaannya hanya untuk kepentingan pekerjaan.

1. Ruang lingkup kebijakan ini mencakup seluruh komponen teknologi informasi properti milik BNPB dan BPBD;
2. Dilarang mempergunakan komputer untuk kepentingan yang tidak terkait dengan kepentingan pekerjaan. Penggunaan komputer untuk kepentingan pribadi diperkenankan namun terbatas dalam pemakaiannya;
3. Pengguna bertanggung jawab terhadap keamanan komputer kerjanya dari kemungkinan kerusakan dan kelalaian penggunaan termasuk penggunaan oleh pihak yang tidak berhak. Pihak yang tidak berhak adalah siapapun pengguna yang tidak diberikan hak akses penggunaan komputer dan tidak mendapatkan ijin tertulis dari pihak pemilk data/informasi dan atau mendapat ijin dari staf pengelola teknologi;
4. Pengguna komputer dilarang mengganti/merubah kata kunci Administrator pada komputernya. Pengguna yang hendak menggunakan hak akses Administrator harus melaporkan kepada staf administrator sistem;
5. Pengelola teknologi akan melakukan pengawasan secara teratur untuk mengaudit penggunaan seluruh komputer yang menjadi tanggung jawabnya. Staf sistem administrator berhak memeriksa/mengakses komputer pengguna tanpa otorisasi/ijin pemilik komputer dalam keperluan yang terkait keamanan komputer dan audit;

6. Pengguna harus memastikan faktor kesehatan kerja guna keselamatan kerja serta menjaga perangkat atas pencurian/kehilangan/kerusakan;
7. Pengguna selain staf sistem administrator dilarang melakukan tindakan yang terkait dengan pekerjaan staf pengelola teknologi sistem administrator, seperti tindakan duplikasi atau hal-hal terkait keamanan komputer;
8. Pengguna dilarang untuk memindahkan, membongkar (sebagian atau keseluruhan) atau melakukan modifikasi (seperti melakukan instalasi perangkat lunak dan perangkat keras tambahan) tanpa persetujuan tertulis dari atasan pengelola teknologi informasi, hal ini adalah untuk menghindari kerusakan komponen teknologi ataupun kehilangan data;
9. Apabila perangkat komputer tidak lagi dipergunakan, baik yang bersifat sementara ataupun permanen, maka perangkat komputer tersebut akan ditarik/dikembalikan dan didistribusikan ulang oleh Biro Umum dibantu staf pengelola teknologi;
10. Pengguna yang meminjam perangkat teknologi bertanggung jawab terhadap keamanan barang yang dipinjamnya dan hanya dipergunakan untuk tujuan yang sesuai dengan tujuan peminjaman serta harus mengembalikan tepat waktu. (Formulir ini dapat dilihat pada **lampiran 12**);
11. Pengguna komputer harus mengaktifkan id dan kata kunci, jika akan mengakses aplikasi atau kejaringan;
12. Seluruh isi data yang tersimpan pada sistem komputer di BNPB dan BPBD akan menjadi hak intelektual BNPB atau BPBD;
13. Ketika akan melakukan perjalanan dengan menggunakan transportasi umum (misal; pesawat terbang, kapal laut) maka perangkat komputer harus tetap dibawa atau tidak disimpan didalam bagasi/koper, kecuali jika ada ketentuan lain dari pihak transportasi, hal ini guna mencegah kehilangan barang, kerusakan, pencurian data dan lain-lain;
14. Seluruh pengguna komputer BNPB dan BPBD bertanggung jawab untuk mematuhi kebijakan ini.

6.2. Pengamanan Area Terbatas

Tujuan kebijakan ini adalah untuk menyediakan perlindungan fisik yang memadai untuk melindungi ruangan-ruangan penting (area terbatas) teknologi informasi terhadap ancaman baik dari manusia maupun alam. (Formulir ini dapat dilihat pada **lampiran 7,8,9,10 dan 11**).

1. Ruang lingkup kebijakan ini mencakup ruangan penyimpanan data, ruang Inventori di BNPB atau BPBD.
2. Akses ke area terbatas hanya diberikan untuk orang-orang tertentu. Daftar individu yang memiliki otorisasi untuk memasuki wilayah terbatas harus ditempel di tempat yang mudah dilihat, dan individu yang tidak terdaftar harus didampingi oleh salah satu dari staf pengelola teknologi informasi yang memiliki otorisasi.

3. Individu yang tidak memiliki otorisasi harus membawa identifikasi berupa dokumen resmi yang diperiksa oleh staf sistem administrator sebelum mereka diijinkan masuk.
4. Log yang mencatat akses ke area terbatas harus tersedia. Pengisian buku catatan harus lengkap termasuk paraf/tandatangan dari staf pengelola teknologi yang bertugas di area terbatas.
5. Area terbatas teknologi informasi dilengkapi dengan kunci untuk membatasi akses, dan alat akses harus diberikan dengan alasan yang jelas (alat akses bisa berupa kunci, kartu magnet, cetak jejak jari atau kombinasi keduanya). Area terbatas harus dilengkapi dengan kamera elektronik untuk keamanan berlapis.
6. Siapapun dilarang makan, minum dan lainnya dalam area terbatas selain kebutuhan untuk pengelolaan sistem teknologi.
7. Siapapun yang membawa barang barang ke dalam dan atau keluar dari area terbatas harus tercatat dalam buku catatan dan harus sepengetahuan staf sistem administrator.
8. Tamu atau pihak ketiga atau vendor yang memiliki keperluan ke dalam area terbatas harus didampingi oleh staf pengelola teknologi. Jika staf tersebut harus meninggalkan ruangan untuk waktu tertentu maka staf harus mencari penggantinya untuk dapat mendampingi tamu/pihak ketiga tersebut, bila tidak memungkinkan penggantinya maka tamu/pihak ketiga tersebut harus keluar dari ruang area terbatas untuk menunggu staf penggati sebagai pendampingnya.
9. Kunci dan atau kartu magnet diberikan sesuai kebutuhan dan dikembalikan jika individu telah keluar/pindah bekerja atau tidak memerlukan akses ke area terbatas tersebut.
10. Kunci kombinasi diubah secara berkala untuk memastikan kombinasi lama yang diketahui oleh mantan karyawan tidak dapat digunakan kembali.
11. Kunci, berupa kartu magnet atau nomor kombinasi untuk masuk ruang penyimpanan data diberikan dengan mengacu pada keamanan kartu yang ditetapkan, termasuk kunci non magnet. Akses hanya diberikan jika memang ada kebutuhan untuk masuk wilayah terbatas.
12. Pintu ruang terbatas seperti penyimpanan data harus selalu terkunci setiap saat.
13. Pengelola teknologi informasi harus menjamin bahwa telah tersedia prosedur-prosedur yang memadai untuk perlindungan terhadap faktor lingkungan (misalnya: kebakaran, debu, tenaga, panas dan kelembaban). Jika memungkinkan dapat juga dipasang peralatan khusus untuk memonitor dan mengendalikan hal tersebut.
14. Standar Kesehatan dan Keselamatan Kerja harus diterapkan dan terpelihara sesuai dengan standar peraturan keselamatan kerja yang berlaku.

15. Seluruh karyawan bertanggung jawab untuk mematuhi kebijakan ini.
16. Pengelola teknologi informasi bertanggung jawab untuk memastikan keamanan dari area terbatas ini.

6.3. Akun Pengguna

Tujuan kebijakan ini adalah untuk mendefinisikan standar pembuatan, perubahan, dan penghapusan akun pengguna (akun pengguna), untuk standar keamanan sistem operasi dan aplikasi di BNPB dan BPBD.

1. Ruang lingkup kebijakan ini berlaku untuk semua pengguna sistem komputer yang beroperasi di BNPB dan BPBD;
2. Semua permintaan untuk memiliki akun harus menggunakan form yang diisi dengan lengkap. Permohonan dapat dipenuhi jika pengisian sudah benar dan lengkap (Formulir ini dapat dilihat pada **lampiran 23**);
3. Staf sistem administrator akan memberikan ijin pembuatan akun pengguna hanya untuk karyawan BNPB dan BPBD. Untuk pihak ketiga akan dibuatkan dengan akun sementara (akun sementara) dan tetap harus dicatat;
4. Aturan Nama user harus :
   a. memiliki format <nama_depan>.<nama_belakang>. misal Arnoldus.Hutapea
   b. bila tidak memiliki “nama belakang” maka diganti dengan 4 digit Nomor Pegawai yang unik
5. Panjang nama minimal 8 karakter (gabungan dari nama depan dan nama belakang);
6. Wewenang pemakaian sistem dibatasi berdasarkan kebutuhan atau permohonan. Pengelola teknologi harus melakukan konfirmasi pada atasan pengguna yang bersangkutan untuk memastikan akses yang diminta memang dibutuhkan pengguna dalam pekerjaannya;
7. Tiap-tiap id-pengguna harus secara unik mengidentifikasi satu pengguna. Id-pengguna yang digunakan bersama atau id-pengguna kelompok tidak diperbolehkan;
8. Semua akses pengguna dihentikan saat individu tersebut berhenti sebagai karyawan BNPB atau BPBD atau waktu yang ditentukan oleh sistem administrator;
9. Pengguna bertanggung jawab atas aktivitas yang dilakukan dengan menggunakan id-pengguna nya;
10. Sistem administrator akan melakukan revisi kembali terhadap akun pengguna dan mengkonfirmasikan hak akses pengguna yang bersangkutan secara berkala;
11. Kebijakan akun pengguna untuk aplikasi kebencanaan harus sesuai dengan kebijakan ini. Akun pengguna untuk aplikasi tetap harus dilakukan meskipun grup jaringan belum menggunakan **nama unik**;
12. Pengelola teknologi informasi bertanggung jawab untuk memastikan

kelayakan akses yang diberikan pada pengguna dan memperhatikan aspek keamanan dalam memberikan akses;

13. Seluruh karyawan dan atau pihak ketiga yang terkait bertanggung jawab untuk mematuhi kebijakan ini;
14. Kebijakan untuk penggunaan akun belum dapat dilaksanakan mutlak hingga kebijakan penggunaan **nama unik** jaringan ditetapkan oleh BNPB namun demikian pengelolaan keamanan jaringan tetap menjadi tanggung jawab seluruh pengelola teknologi informasi.

6.4. Perlindungan Terhadap Virus

Tujuan kebijakan ini adalah untuk memastikan sistem komputer BNPB dan BPBD terlindung dari serangan virus dan pencegahan yang berkesinambungan.

1. Ruang lingkup kebijakan ini berlaku atas semua komputer dan jaringan di BNPB dan BPBD (seperti komputer, penyimpanan data dan perangkat berbasis komputer lainnya). Kebijakan ini berlaku mutlak setelah BNPB memiliki anti virus standar, namun tindakan pencegahan tetap mengacu pada kebijakan ini;
2. Seluruh perangkat komputer harus memiliki piranti lunak antivirus yang terkini yang diaktifkan secara teratur;
3. BNPB dan BPBD harus memiliki program perangkat lunak anti virus standar berlisensi;
4. Menduplikasi pada penyimpanan data harus dijadwalkan untuk dilakukan minimal satu kali dalam seminggu;
5. Piranti lunak anti virus dan solusi virus harus selalu diperbaharui. Bagian Teknologi melalui staf teknologi informasi akan melakukan instalasi antivirus dan mendistribusikannya secara teratur;
6. Pengguna harus memutuskan hubungan jaringan komputernya dari jaringan internal komunikasi data ketika mencurigai bahwa terdapat virus pada komputernya, dan harus segera melaporkan kepada staf pengelola teknologi informasi guna meminimalkan dampak dan mencegah virus menyebar di dalam jaringan;
7. File yang diperoleh dari luar yang mungkin mengandung virus (misalnya lampiran dari surat elektronik, disc ataupun virus dari media disk) harus diperiksa dengan anti virus lebih dahulu;
8. Pengguna komputer jinjing harus memastikan bahwa perangkat tersebut telah bebas dari virus (melalui sistem deteksi) sebelum terhubung kedalam jaringan. Apabila terdapat keraguan, pengguna tersebut harus meminta bantuan dari staf pengelola teknologi;
9. Tamu yang mempergunakan komputer jinjing harus melaporkan perangkat mereka kepada staf pengelola teknologi sebelum terhubung kedalam jaringan, dan staf pengelola teknologi harus memastikan bahwa perangkat tersebut telah bebas dari virus;
10. Pengguna harus menghindari akses penggunaan bersama terhadap

media penyimpanan, misal media disket dengan akses baca / tulis (baca/tulis) dan hanya diperkenankan jika sudah dipastikan kemanan data dan media tersebut.

11. Pengguna dilarang melakukan pengambilan file dari internet, membuka file ataupun makro yang terdapat pada surat elektronik yang berasal dari sumber yang tidak diketahui ataupun mempergunakan media disket dari sumber yang tidak diketahui;
12. Pengguna dilarang membuat dan atau mendistribusikan program-program perusak ke dalam jaringan (contoh: virus);
13. Seluruh karyawan dan atau pihak ketiga yang terkait bertanggung jawab untuk memastikan keamanan penggunaan fasilitas teknologi informasi di jaringan BNPB dan BPBD dan harus mematuhi kebijakan ini;
14. Pengelola teknologi informasi BNPB dan BPBD bertanggung jawab untuk menyediakan dan mendistribusikan piranti lunak antivirus terbaru pada semua komputer yang terhubung dengan jaringan BNPB dan BPBD serta memastikan adanya pendeteksian dan tindakan pencegahan terhadap virus.

6.5. Kata kunci

Tujuan kebijakan ini adalah untuk memastikan bahwa akses terhadap informasi data diatur secara tepat dan memadai untuk mencegah hilangnya data, informasi dan kerahasiaan data, yang disebabkan akses oleh pihak-pihak yang tidak mempunyai otorisasi.

1. Ruang lingkup kebijakan ini berlaku mutlak bagi semua pengguna sistem informasi di BNPB dan BPBD baik aplikasi dan sistem operasi.
2. Pengguna bertanggung jawab atas semua aktivitas yang dilakukan dengan menggunakan id-pengguna dan kata kunci-nya.
3. Pengguna harus menggunakan kata kunci untuk masuk ke dalam sistem komputer dan memastikan kata kunci diganti secara berkala.
4. Semua kata kunci harus dirahasiakan; jika tertulis maka kata kunci harus tetap dirahasiakan dan disimpan di tempat yang aman, yang tidak bisa diakses orang lain.
5. Kata kunci awal yang dikeluarkan oleh staf sistem administrator harus diubah pengguna pada sesi langsung pertama. Mengelola kata kunci (misalnya: kata kunci yang dibuat oleh mitra saat instalasi sistem pertama kali) harus segera diganti.
6. Semua kata kunci pada level pengguna (misalnya; surat elektronik, internet, komputer kerja) harus mematuhi ketentuan berikut.
   a. Panjang kata kunci minimal = 8 karakter
   b. Umur kata kunci maksimal = 60 hari
   c. Umur kata kunci minimal = 1 hari
   d. Riwayat kata kunci = 9 kali
   e. Mempergunakan kombinasi huruf dan angka

7. Semua kata kunci pada level sistem (misalnya; sistem akun administrator, akun aplikasi) harus mematuhi ketentuan berikut.
   a. Panjang kata kunci minimal = 8 karakter
   b. Umur kata kunci maksimal = 30 hari
   c. Umur kata kunci minimal = 1 hari
   d. Riwayat kata kunci = 12 kali
   e. Mempergunakan kombinasi huruf dan angka
8. Setelah 3 kali gagal memasukkan kata kunci maka id-pengguna akan dinonaktifkan oleh sistem. Pengguna harus segera menghubungi staf sistem administrator.
9. Semua kata kunci harus segera diubah jika diduga atau diketahui kata kunci tersebut telah diketahui oleh pihak yang tidak memiliki otorisasi.
10. Kata kunci tidak boleh digunakan bersama atau diberitahukan pada orang lain selain pengguna yang memiliki otorisasi. Tidak dibenarkan untuk mencatat dan menyimpan kata kunci dalam bentuk teks file ataupun dokumen asli dan meletakkannya dalam lingkungan yang dapat dilihat dengan jelas oleh orang yang tidak memiliki otorisasi.
11. Seluruh pengguna bertanggung jawab untuk memastikan keamanan penggunaan id-pengguna dan kata kunci-nya, berikut aktivitas yang dilakukan dengan menggunakan id-pengguna dan kata kunci-nya pada pekerjaannya.
12. Staf sistem administrator diperkenankan menyimpan informasi kata kunci dari pengguna (setelah mendapat ijin dari pengguna) untuk keperluan perbaikan sistem pada komputer pengguna.
13. Staf sistem administrator harus mencatat semua id-pengguna dan kata kunci pada sistem penyimpanan data dan sistem operasi serta disimpan dalam amplop tertutup untuk dikuasakan kepada pimpinan pengelola teknologi jika dibutuhkan sewaktu-waktu, terutama hal-hal yang mendesak atau urgen.
14. Staf sistem administrator bertanggung jawab untuk memastikan keamanan kata kunci pada level sistem.
15. Kebijakan kata kunci untuk jaringan akan disesuaikan dengan diberlakukannya sistem nama unik di BNPB.

6.6. Penggunaan Informasi Dan Data

Tujuan kebijakan ini adalah untuk memastikan informasi dan data digunakan dengan benar dan hanya untuk kepentingan BNPB dan BPBD.

1. Ruang lingkup kebijakan ini berlaku atas semua pengguna sistem informasi di BNPB dan BPBD.
2. Pengguna dilarang menggunakan informasi yang tersedia di sistem untuk tujuan tak resmi, keuntungan pribadi atau digunakan secara tak resmi oleh pihak lain termasuk mengungkapkan dan menyediakan akses

untuk data atau informasi bagi orang-orang yang tidak memiliki otorisasi.

3. Pengguna bertanggung jawab dalam menggunakan informasi dan data milik BNPB atau BPBD dan harus menghargai informasi tersebut sebagai aset milik BNPB dan BPBD.
4. Seluruh pengguna yang menggunakan dan memproses informasi dan data bertanggung jawab untuk segala resiko dan tindakan pengamanan yang berkaitan dengan informasi dan data tersebut.
5. Seluruh pengguna dan atau pihak ketiga yang terkait bertanggung jawab untuk memastikan kelayakan dan keamanan penggunaan fasilitas sistem informasi BNPB dan BPBD serta wajib mematuhi kebijakan ini.

6.7. Mengakses Jarak Jauh dan Jaringan Tanpa Kabel

Tujuan kebijakan ini adalah untuk meminimalkan kemungkinan resiko kerusakan pada jaringan informasi, yang disebabkan oleh pengunaan peralatan komputer yang tidak terotorisasi. Kerusakan mencakup kehilangan data penting, cemarnya nama baik BNPB atau BPBD di masyarakat, atau kerusakan pada sistem internal dan lainnya.

1. Ruang lingkup kebijakan ini mencakup semua koneksi jaringan sistem informasi di BNPB dan BPBD termasuk akses ke telekomunikasi, data, file dan aplikasi.
2. Jaringan informasi hanya dipergunakan untuk kepentingan BNPB dan BPBD. Aktivitas untuk tujuan lainnya tidak dibenarkan.
3. Pengguna akses jarak jauh harus mempergunakan koneksi yang terenkripsi kedalam jaringan BNPB atau BPBD ketika terhubung dengan jaringan secara mengakses dengan jarak jauh.
4. Fasilitas akses jarak jauh ini dipergunakan untuk membantu pekerjaan terkait guna mendukung fungsi-fungsi di bawah tanggung jawabnya.
5. Pengguna selain staf sistem administrator dilarang melakukan koneksi akses jarak jauh kedalam penyimpanan data kecuali telah memilki ijin tertulis dari staf sistem administrator dan hanya terkait untuk kepentingan pekerjaannya serta memberikan alasan yang rasional dan dibenarkan oleh pengelola teknologi informasi.
6. Dilarang mempergunakan alat koneksi internet eksternal ke dalam komputer atau penyimpanan data ketika komputer atau penyimpanan data tersebut sedang terhubung dengan jaringan.
7. Dilarang menghubungkan perangkat berbasis komputer ke dalam jaringan selain perangkat berbasis komputer yang telah diotorisasi dan didaftarkan oleh pengelola teknologi informasi (missal : komputer pribadi, telepon pintar pribadi dan lain-lain).
8. Instalasi dan penggunaan jaringan nirkabel pada jaringan tidak diperkenankan kecuali dengan persetujuan tertulis dari staf sistem administrator. Staf sistem administrator harus mengambil langkah pengamanan guna mencegah kemungkinan penyalahgunaan koneksi nirkabel tersebut.

9. Perlindungan atas informasi dalam koneksi jaringan merupakan tanggung jawab semua pengguna yang memanfaatkan koneksi nirkabel atau akses jarak jauh.
10. Seluruh karyawan dan atau pihak ketiga yang terkait harus mematuhi kebijakan ini.

6.8. Operasional Teknologi Informasi Dalam Keadaan Darurat

Tujuan kebijakan ini adalah untuk memberikan panduan atas usaha-usaha pengamanan di lokasi kantor BNPB atau BPBD serta pembuatan rencana tentang prosedur dan lokasi operasi alternatif jika terjadi gangguan terhadap operasional di lingkungan BNPB dan BPBD.

1. Ruang lingkup kebijakan ini berlaku untuk semua operasi darurat teknologi di lingkungan BNPB dan BPBD.
2. Rencana tertulis harus disusun untuk memastikan pulihnya layanan-layanan informasi darurat saat terjadi gangguan besar. Rencana tersebut harus memuat:
   a. Identifikasi program aplikasi kritis, sistem operasi, sumber daya manusia, persediaan barang, file data, dan jangka waktu yang dibutuhkan untuk pemulihan setelah gangguan terjadi.
   b. Identifikasi prioritas dan prosedur untuk pengoperasian kembali program-program aplikasi kritis/sensitif tertentu, dan pemulihan kembali jaringan informasi serta telekomunikasi.
   c. Prosedur dan jangka waktu yang berbeda untuk tingkat gangguan yang berbeda, untuk memastikan respon yang sesuai bagi tiap-tiap kasus.
   d. Alternatif prosedur pemrosesan untuk id pengguna alternatif-alternatif lokasi cadangan dan perangkat keras, serta alternatif yang dipilih dari semua alternatif yang ada.
   e. Rencana dan prosedur untuk memulai kembali operasi normal setelah lokasi teknologi informasi yang rusak telah selesai diperbaiki.
   f. Prosedur rekonstruksi dan operasi pada lokasi cadangan.
   g. Lebih dari satu sumber barang-barang kebutuhan, termasuk persediaan formulir-formulir khusus, untuk digunakan dalam pemulihan layanan setelah terjadinya gangguan.
3. Pengoperasian perangkat teknologi akan diatur dengan tindakan-tindakan pengamanan yang memadai, yang dirancang untuk mencegah terjadinya gangguan operasi karena api, pengaruh cuaca buruk, atau air.
4. Pengguna harus bertindak hati-hati dan bertanggung jawab jika terjadi hal-hal yang tidak diinginkan. Pengguna harus meminta bantuan kepada pengelola teknologi informasi jika mengalami kesulitan dengan fasilitas teknologi yang dipergunakan.
5. Semua Pengguna bertanggung jawab untuk menyampaikan isu atau kekuatiran yang berhubungan dengan kelanjutan operasional teknologi

informasi di area/daerahnya.

6. Untuk tindakan penanganan darurat terhadap infrastruktur teknologi, maka pengelola teknologi informasi harus melakukan pengujian secara berkala pada prosedur dilokasi yang telah ditentukan. Semua pihak yang berkepentingan harus mengikuti pelatihan tentang pengujian ini.
7. Pengelola teknologi informasi bertanggung jawab untuk membuat dan melaksanakan rencana operasi berkelanjutan atas fungsi-fungsi kritis selama keadaan darurat serta memastikan bahwa rencana pelaksanaannya efektif, dan selalu diperbarui.
8. Seluruh pengguna yang mengoperasikan fasilitas teknologi informasi harus mematuhi kebijakan ini.

6.9. Perlindungan Sistem Teknologi Informasi

Tujuan kebijakan ini adalah untuk memberikan panduan perlindungan sistem teknologi informasi secara umum pada jaringan di lingkungan BNPB dan BPBD.

1. Ruang lingkup kebijakan ini berlaku untuk semua sistem komputer dan jaringan di BNPB dan BPBD.
2. Semua kata kunci tingkat pengguna dan administrator harus dibuat kompleks. Semua interaksi dengan penyimpanan data harus dilakukan dengan menggunakan personal id-pengguna. Penggunaan akun standar sistem (seperti “pengguna” atau “administrator”) diperbolehkan hanya bila secara teknis tidak dimungkinkan.
3. Staf sistem administrator harus membuatkan daftar satu perintah yang boleh/dapat diakses oleh pengguna. Pengguna dilarang mengakses satu perintah selain dari satu perintah yang sudah ditentukan
4. Semua tingkatan tambalan harus selalu diperbarui, terutama di komputer yang memuat layanan umum dan bisa diakses lewat sistem lalu lintas jaringan komputer surat, dan layanan DNS.
5. Semua layanan di sistem yang tidak dibutuhkan harus dimatikan atau dibuat tidak aktif, untuk menghilangkan atau meminimalkan jalan masuk serangan.
6. Peralatan cadangan untuk perangkat pembagian protokol dan penghubung jaringan harus tersedia. Semua yang terkait dengan komponen jaringan (konektor, piranti lunak manajemen jaringan dan lainnya) harus terlindung dari kemungkinan akses yang tidak terotorisasi.
7. Semua aktivitas spam, junk surat elektronik, surat elektronik-surat elektronik yang berisi lampiran file yang umumnya dipakai untuk menyebarkan virus, program-program perusak, program setara virus harus dihalangi di penyimpanan data gateway.
8. Staf sistem administrator harus memastikan hal-hal sebagai berikut.
   a. bahwa definisi virus ditempatkan di penyimpanan data sekali seminggu, kecuali jika ada penyebaran virus besar-besaran. Setiap

penyimpanan data harus di scan minimal satu minggu sekali.

b. Bahwa disk perbaikan darurat untuk setiap penyimpanan data utama, tersedia secara teratur, berguna untuk menghindari masalah keamanan sistem.

c. Pelanggaran dan aktivitas yang berhubungan dengan keamanan sistem dicatat, ditelaah, dan dieskalasi secara berkala untuk mengidentifikasi dan menyelesaikan insiden yang melibatkan aktivitas tak terotorisasi.

9. Staf sistem administrator bertanggung jawab untuk mengelola tindakan pengamanan sesuai dengan kebutuhan sistem.

10. Seluruh pengguna dan atau pihak ketiga yang terkait, bertanggung jawab untuk melakukan tingkat keamanan yang memadai serta wajib mematuhi kebijakan ini.

BAB VII
PELAPORAN

7.2 Pelaporan

Pelaporan dalam aplikasi sistem informasi kebencanaan secara umum adalah penyampaian informasi yang telah dimasukkan dan diolah secara komputerisasi. Penyampaian informasi bisa dilakukan melalui media tercetak atau elektronik. Pelaksanaannya adalah dengan memberikan laporan rutin kepada internal BNPB dan BPBD atas kuantitas dan kualitas data kebencanaan pada setiap bulannya.

Komponen informasi pelaporan yang dibuat minimal harus memiliki informasi sebagai berikut.

a. Perangkat keras (misal; kapasitas penyimpanan sekunder, Penambahan perangkat teknologi dan lain-lain).
b. Perangkat lunak (missal : penambahan perangkat lunak, penambahan akun dan lain-lain).
c. Pelayanan permasalahan teknologi informasi (misal: jumlah problem dan solusinya).
d. Isu lain (misal: virus, bimbingan teknis dan lain-lain).

7.3 Penyalahgunaan dan Pelanggaran

Bagian terpenting didalam pelaksanaan Peraturan Kepala ini khususnya untuk segala kebijakan yang terkait dengan penggunaan teknologi informasi yang berada dilingkungan BNPB dan BPBD adalah komitmen bagi seluruh pejabat dan pengelola teknologi informasi dalam menegakan kebijakan internal dilingkungannya. Kategori jenis pelanggaran mempertimbangkan faktor resiko keamanan sistem informasi kebencanaan yang dapat berakibat pada data dan informasi internal maupun eksternal di BNPB dan BPBD. Penyalahgunaan dan atau pelanggaran terhadap Peraturan Kepala ini akan diselesaikan melalui peraturan yang berlaku di BNPB dan BPBD.

7.4 Evaluasi

Evaluasi dalam sistem informasi kebencanaan adalah proses verifikasi dan analisa terhadap efektifitas penggunaan infrastruktur dan sistem informasi kebencanaan termasuk penilaian kuantitas dan kualitas data yang telah direkam ke dalam sistem informasi kebencanaan. Evaluasi sistem informasi kebencanaan secara umum dapat dilakukan sebagai berikut.

1. Evaluasi terhadap penggunaan sistem informasi kebencanaan dilakukan secara berkesinambungan, sesuai dengan masukan baik dari BNPB maupun dari BPBD.
2. Evaluasi kesesuaian antara sistem aplikasi dan infrastruktur teknologi informasi BNPB dilakukan setiap tiga bulan sekali.

3. Evaluasi terhadap seluruh kebutuhan infrastruktur dan termasuk seluruh sistem aplikasi harus terus dikembangkan dan disesuaikan dengan kebutuhan rencana strategi BNPB.

BAB VIII
PENUTUP

Pedoman Peraturan Kepala tentang teknologi informasi BNPB ini disusun sebagai standar kebijakan di BNPB dan BPBD dalam rangka pemanfaatan secara optimal komponen infrastruktur termasuk seluruh aplikasi kebencanaan agar lebih terintegrasi dan terpadu untuk mendukung usaha penanggulangan kebencanaan, yang merupakan amanat dari Presiden Republik Indonesia.

KEPALA BADAN NASIONAL
PENANGGULANGAN BENCANA

SYAMSUL MAARIF

DAFTAR ISTILAH

Istilah	Keterangan
Bridge	Penghubung yang terdiri dari dua port
DHCP	Dinamis Konfigurasi Host Protokol yaitu untuk memudahkan pengalokasian alamat IP dalam satu jaringan. Semua komputer yang tersambung di jaringan akan mendapatkan alamat IP secara otomatis dari penyimpanan data DHCP.
DNS	Nama unik, adalah sebuah sistem yang menyimpan informasi tentang nama host maupun nama nama unik dalam bentuk basis data tersebar di dalam jaringan komputer yang berfungsi untuk mengerjakan pengalamatan dan penjaluran.
Nama unik	nama unik yang diberikan untuk mengidentifikasi nama penyimpanan data komputer seperti web penyimpanan data atau surat elektronik penyimpanan data di internet.
Surat elektronik	Surat elektronik
Surat elektronik Bomb	Surat elektronik berisi kode program yang akan menularkan kedalam sistem komputer dengan cara mengambil semua alamat surat elektronik yang ada didalam komputer untuk dikirimkan kembali informasi surat elektronik ini berulang-ulang. Bisa menurunkan kinerja komputer
Disket Perbaikan Darurat	sebuah disket floppy yang diformat secara khusus yang tidak dapat digunakan untuk melakukan proses booting yang mengandung informasi mengenai konfigurasi dasar sistem operasi, digunakan untuk memulihkan komputer sehingga mampu melakukan proses booting kembali
Proses Transformasi	proses untuk “mengaburkan” informasi untuk membuat informasi tersebut tidak bisa dibaca tanpa pengetahuan khusus.
Hub / repeater	perangkat yang memiliki banyak port yang berfungsi menghubungkan serta mengatur beberapa komputer untuk membentuk suatu jaringan pada topologi star.
Pusat Kontak	Pusat Pelayanan permasalahan teknologi informasi di

Teknologi Informasi	BNPB
Jaringan komunikasi data	Media jalur data baik fisik dan digital menggunakan konsep teknologi IP (Internet Protokol) yang disediakan BNPB, BPBD
Macro	kode program yang biasa dibuat dalam bahasa Visual Basic. Macro ini biasanya akan dianggap program yang sudah terotorisasi oleh sistem dan dijalankan secara tersembunyi tanpa sepengetahuan pengguna. Macro virus dapat berjalan dibanyak aplikasi seperti microsoft office.
Pengelola teknologi / Pengelola teknologi informasi	Staf teknologi informasi Bidang Informasi di Pusdatinmas BNPB atau tenaga teknologi informasi di unit-unit di BPBD dibawah Sekretariat
Pihak ketiga	Orang atau badan atau organisasi yang sedang berafiliasi bekerjasama dengan BNPB/BPBD. Tamu kunjungan dan vendor/konsultan juga bahagian dari pihak ketiga
Port	suatu celah atau pintu atau lubang pada system komputer sebagai jalur transfer data. Dua jenis port yakni jenis fisik dan virtual.
Router	sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau Internet
SLO	Standar Lingkungan Operasi
SINDU	Sistem Informasi Kebencanaan Terpadu. Sebuah sistem aplikasi yang ditetapkan sebagai standar utama untuk aplikasi kebencanaan bagi BNPB dan BPBD.
SPAM	surat elektronik yang tidak diinginkan oleh pengguna fasilitas komputer dalam bentuk surat elektronik, dan lain-lain. SPAM biasanya berisi iklan dari perusahaan yang mengakibatkan ketidaknyamanan bagi pengguna.
Switch	perangkat keras seperti hub yakni distribusi packet data antar komputer dan hanya akan mengirimkannya ke komputer yang berkepentingan menerima data atau Bridge yang terdiri dari banyak port.
Sistem	Staf Sistem Administrasi jaringan dan infrastruktur

Administrator	informasi teknologi
Virus	program independen yang menyalinkan dirinya sendiri menjadi banyak didalam sistem komputer. Bisa merusak, merubah atau menurunkan kinerja sistem dengan memanfaatkan sumber daya seperti memori atau harddisk.
Grup Kerja	Pengelompokkan komputer jaringan yang berperan sebagai peer dan tidak ada kontrol atas masing-masing komputer.
Virus	program yang menyalinkan dirinya sendiri dengan berulang-ulang, sistem ke sistem, dengan menggunakan sumber daya dan dapat memperlambat kinerja sistem.

DAFTAR LAMPIRAN

LAMPIRAN 1. STANDARD PERANGKAT LUNAK APLIKASI UNTUK KOMPUTER DESKTOP/NOTEBOOK/LAPTOP

Nama Aplikasi	Deskripsi	Versi	Vendor	Tipe Lisensi
Microsoft Windows 2010Professional	Operating Systems	SP 4	Microsoft	Volume License (number of installation+ CAL)
Microsoft Office 2007 Standard: - Microsoft Word - Microsoft Excell - Microsoft Powerpoint - Microsoft Outlook	Standard Office Applications	Standard	Microsoft	Volume License (number of installation)
Internet Explorer	Browser	9 SP1	Microsoft	Included in Operating System
Anti Virus Client	Norton Anti Virus Enterprise	Last version 2012	Symantec	Number of installation
Acrobat Reader	PDF reader	8	Adobe	Free
Microsoft Windows XP	Operating Systems	SP 3	Microsoft	Volume License (number of installation + CAL)
Microsoft Windows 7	Operating Systems	7	Microsoft	Volume License (number of installation + CAL)

LAMPIRAN 2. OPSIONAL PERANGKAT LUNAK APLIKASI TAMBAHAN UNTUK KOMPUTER DESKTOP/NOTEBOOK/LAPTOP

Nama Aplikasi	Deskripsi	Versi	Vendor	Tipe Lisensi
Mozila Firefox	Browser	8	Mozila	Free
Microsoft Project 2007	Project Management	2007	Microsoft	Number of installation
Microsoft Visio Professional	Flow charter	2007	Microsoft	Number of installation
Microsoft Anti Spyware	Antispyware for Internet Users	Beta1	Microsoft	Free
Microsoft Office 2007 Professional: - Microsoft Access - Microsoft Powerpoint	Pro version of Office	2007	Microsoft	Number of installation

LAMPIRAN 3. STANDAR PERANGKAT LUNAK APLIKASI SISTEM INFORMASI KEBENCANAAN

Nama Aplikasi	Deskripsi	Versi	Sumber	Tipe Lisensi
SINDU (Sistem Informasi Kebencanaan Terpadu)	Digunakan tahun 2013	1.0	Internal IT Pusdatinmas BNPB	

LAMPIRAN 4. STANDAR PERANGKAT LUNAK APLIKASI SISTEM INFORMASI UMUM (NON KEBENCANAAN)

Nama Aplikasi	Deskripsi	Versi	Sumber	Tipe Lisensi

LAMPIRAN 5. STANDAR PERANGKAT KERAS UNTUK KOMPUTER DESKTOP/NOTEBOOK/LAPTOP

Item	Minimal Spesifikasi
Processors	1 GHz (x86 processor) dan 1.4 GHz (x64 processor)
RAM / memori	512 MB
Ethernet	10/100 mbps
I/O Ports	6 x USB 2.0 serial, pararel, estate , WLAN, Etheernet ri – 45
Hard-disk	10 GB
Optical drive	DVD/VCD/ combo derive
Monitor	Super VGA (800 x 600) or higher-resolution monitor – merk harus sama dengan CPU
Keyboard	US 101
Mouse	Scroll 3 buttons
Garansi	Complete

LAMPIRAN 6. STANDAR PERANGKAT KERAS UNTUK KOMPUTER PENYIMPANAN DATA

Item	Minimal Spesifikasi
Processors	2 GHz (x86 processor) , FSB1066, I2 Cache 1 mb 2 GHz (x64 processor), FSB1066, I2 Cache 1 mb
RAM / memori	4 GBDDR2PC 5300
Ethernet	10/100 mbps
I/O Ports	6 x USB 2.0 serial, pararel, estate , WLAN, Etheernet ri – 45
Hard-disk	40 GB
Optical drive	DVD/VCD/ combo derive
Monitor	Super VGA (800 x 600) or higher-resolution monitor – merk harus sama dengan CPU
Keyboard	US 101
Mouse	Scroll 3 buttons
Garansi	Complete

LAMPIRAN 7. BUKU CATATAN PENYIMPANAN RUANG DATA

BNPB

Log Book Server Room

Badan Nasional Penanggulangan Bencana
Pusat Data Informasi dan Humas
Floor 4, Gedung BNPB
J. Ir. H. Juanda No. 36,Jakarta Pusat, Indonesia
Phone: (021) 3442734, 3442985, 3443079
Facsimile: (021) 3505075

Form No. 01-01

LOCATION : H.O. JAKARTA

Day	Date	Full Name	Organization / Unit	Accompanied by	Purpose	Time In	Sign	Time Out	Sign

All users must full-fill this book before and after enter to room server
Completed by each individual who enters and exits - Maximum stay by visitor is three minutes - Maximum visitors per entry is less than number of staff - Keep door closed

Acknowledged,	Acknowledged,
Date :	Date :
ICT Administrator	ICT Manager

CONFIDENTIAL DOCUMENT - TO BE FILLED BY ICT ADMINISTRATOR - DO NOT PHOTO-COPY WITHOUT CONSENT FROM HEAD OF INFORMATION DIVISION

LAMPIRAN 8. REKAP PENYIMPANAN INVENTARIS RUANG DATA

BNPB

Server Room Inventory

Badan Nasional Penanggulangan Bencana
Pusat Data Informasi dan Humas
Floor 4, Gedung BNPB
Jl. Ir. Hj. Juanda No. 36, Jakarta Pusat, Indonesia
Phone: (021) 3442734, 3442985, 3443079
Facsimile: (021) 3505075

Form No. 01-02

LOCATION : H.O. JAKARTA

Day	Date	Name (brand/model/serial)	Quantity	Accompanied by	From	To	Recorded by	Purpose

Completed by ICT Administrator - Use this log as needed - Report to ICT Manager when columns full

Acknowledged, Date : _____	Acknowledged, Date : _____
_____ ICT Administrator	_____ ICT Manager

CONFIDENTIAL DOCUMENT - TO BE FILLED BY ICT ADMINISTRATOR
DO NOT PHOTO-COPY WITHOUT CONSENT FROM HEAD OF INFORMATION DIVISION

LAMPIRAN 9. REKAP PENYIMPANAN INTEGRITAS RUANG DATA

BNPB

Server Room Integrity

Badan Nasional Penanggulangan Bencana
Pusat Data Informasi dan Humas
Floor 4, Gedung BNPB
Jl. Ir. Hj. Juanda No. 36,Jakarta Pusat, Indonesia
Phone: (021) 3442734, 3442665, 3443079
Facsimile: (021) 3505075

Form No. 01-05

LOCATION : H.O. JAKARTA

Day	Date	Time (24)	Room No.	Temperature (C)	Humidity (%)	Floor	Walls	Ceiling	Record by

Completed by ICT Administrator - Executed every beginning, middle, and end of each shift or day

Acknowledged,	Acknowledged,
Date : _____	Date : _____
_____	_____
ICT Administrator	ICT Manager

CONFIDENTIAL DOCUMENT - TO BE FILLED BY ICT ADMINISTRATOR
DO NOT PHOTO-COPY WITHOUT CONSENT FROMHEAD OF INFORMATION DIVISION

LAMPIRAN 10. REKAP BATERAI, PENYIMPANAN DATA AND PENGHUBUNG SISTEM

BNPB

Log Batteries, Servers and Switches

Badan Nasional Penanggulangan Bencana
Pusat Data Informasi dan Humas
Floor 4, Gedung BNPB
Jl. Ir. Hj. Juanda No. 36,Jakarta Pusat, Indonesia
Phone: (021) 3442734, 3442985, 3443079
Facsimile: (021) 3505075

Form No. 01-04

LOCATION : H.O. JAKARTA

Day	Date	Name (brand/model/serial)	Quantity	Accompanied by	From	To	Recorded by	Purpose

Completed by ICT Administrator - Use this log as needed - Report to ICT Manager when columns full

Acknowledged, Date : _____	Acknowledged, Date : _____
_____ ICT Administrator	_____ ICT Manager

CONFIDENTIAL DOCUMENT - TO BE FILLED BY ICT ADMINISTRATOR
DO NOT PHOTO-COPY WITHOUT CONSENT FROM HEAD OF INFORMATION DIVISION

LAMPIRAN 11. PENYIMPANAN BUKU TAMU RUANG DATA

BNPB

SERVER ROOM GUEST BOOK

Badan Nasional Penanggulangan Bencana
Pusat Data Informasi dan Humas
Floor 4, Gedung BNPBJL. Ir. H. Juanda No. 36
Jakarta Pusat. Indonesia
Telp. (021) 3442734, 3442985, 3443079
Fax. (021) 3505075

CONFIDENTIAL DOCUMENT - TO BE FILLED BY IT ADMINISTRATOR
DO NOT PHOTO-COPY WITHOUT CONSENT FROM HEAD OF INFORMATION DIVISION

Form No. 01-05 **LOCATION : H.O. JAKARTA**

NO	Date	Full Name	INTERNAL/ EKSTERNAL	Purpose	TIME IN (Hour : Minute)	SIGN	TIME OUT (Hour : Minute)	SIGN	REMARK

Acknowledge by,
Date : _____

File Version : 01-1

LAMPIRAN 12. DAFTAR PINJAMAN PERALATAN

BNPB

List of Lending Equipment

Badan Nasional Penanggulangan Bencana
Pusat Data Informasi dan Humas
Floor 4, Gedung BNPB
Jl. Ir. H. Juanda No. 36,Jakarta Pusat, Indonesia
Phone: (021) 3442734, 3442985, 3443070
Facsimile: (021) 3000070

User Name : _____ Purpose : _____

Division : _____ Date Return : _____

Form No. 01-06

LOCATION : H.O. JAKARTA

No	Equipment	Serial No	Description of equipment	Sign

Completed by ICT Administrator - Executed every beginning, middle, and end of each shift or day

Acknowledged, Date :	Acknowledged, Date :
ICT Administrator	ICT Manager

CONFIDENTIAL DOCUMENT - TO BE FILLED BY ICT ADMINISTRATOR
DO NOT PHOTOCOPY WITHOUT CONSENT FROM HEAD OF INFORMATION DIVISION

LAMPIRAN 13. KEHILANGAN DAN KERUSAKAN DARI LAPORAN PEMINJAMAN

BNPB

Badan Nasional Penanggulangan Bencana
Pusat Data Informasi dan Humas
Floor 4, Gedung BNPBJL. Ir. H. Juanda No. 36
Jakarta Pusat. Indonesia
Telp. (021) 3442734, 3442985, 3443079
Fax. (021) 3505075

CONFIDENTIAL DOCUMENT - TO BE FILLED BY IT ADMINISTRATOR
DO NOT PHOTO-COPY WITHOUT CONSENT FROM HEAD OF INFORMATION DIVISION

MISSING AND DAMAGE REPORT FORM

Req. No :	**Cost Center :**
Req Date :	**Department :**
User Name :	**Location :**

☐ MISSING ☐ DAMAGE

SOFTWARE;
- ☐ OPERATING SYSTEMS
- ☐ BUSINESS APPLICATION
- ☐ E-MAIL APPLICATION
- ☐ CASE TOOLS
- ☐ OTHER ; _____

COMMUNICATION;
- ☐ PHONE HANDSET
- ☐ HAND PHONE
- ☐ RADIO
- ☐ PAGER
- ☐ BATTERY/CHARGER
- ☐ PABX
- ☐ OTHER ; _____

COMPUTER & PERIPHERAL;
- ☐ CPU
- ☐ MONITOR
- ☐ KEYBOARD
- ☐ MOUSE
- ☐ MOUSE PAD
- ☐ PROCESSOR
- ☐ RAM
- ☐ HARDDISK
- ☐ FLOPPY DISK DRIVE
- ☐ CD-ROM
- ☐ PRINTER
- ☐ PCMCIA CARD
- ☐ DATA CABLE
- ☐ POWER CABLE
- ☐ POWER ADAPTOR
- ☐ HAND HEALD
- ☐ NETWORK CARD
- ☐ CABLE
- ☐ ZIP DRIVE
- ☐ JAZZ DRIVE
- ☐ TAPE BACKUP
- ☐ OTHER ; _____

PLEASE SPECIFY DETAIL REASON :

_____

_____

Requestor Only

_____
Requestor

_____
Requestor's MANAGER

Specification Things :

Information Services Only

Manufacture/Brand Name : _____

Serial Number : _____

Other Specification : _____

Recipient name : _____

Date Received : _____

Approved by,

Altos Febrianto
Information Services Manager

Checked by,

SECTION HEAD SIGNATURE

Note :

_____

_____

_____

LAMPIRAN 14. BERITA ACARA KEHILANGAN BARANG

Badan Nasional Penanggulangan Bencana
Pusat Data Informasi dan Humas
Floor 4, Gedung BNPBJL. Ir. H. Juanda No. 36
Jakarta Pusat. Indonesia
Telp. (021) 3442734, 3442985, 3443079
Fax. (021) 3505075

BERITA ACARA KEHILANGAN BARANG

Pada hari ini .....tanggal ..... bulan ..... tahun dua ribu.
Telah terjadi kehilangan barang berupa : .....
.....
.....
Dengan nomor asset : .....
Type : .....
Merk : .....
Tahun Pembuatan : .....
Dengan penjelasan sebagai berikut : .....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Departement .....
Pelapor

Mengetahui Manager

(.....)

(.....)

Form No. 01-08

LAMPIRAN 15. DETAIL CATATAN APLIKASI LAYANAN UNTUK PENGEMBANG

BNPB

Log Application Service Details for Developers

Badan Nasional Penanggulangan Bencana
PUSDATINMAS, Floor 4, Gedung BNPB
Jl. Ir. H. Juanda No. 36 Jakarta Pusat, Indonesia
Phone: (021) 3442734, 3442985, 3443079
Facsimile: (021) 3505075

Form No. 02-01

LOCATION : H.O. JAKARTA

Application Service Name	Physical Location	Public IP	Private IP	Port(s)	Username(s)	Password(s)	Status

STRICTLY CONFIDENTIAL - Completed by ICT Administrators - To be used only by authorized application developers - Authorization by Head of Information Division

Acknowledged, Date :	Acknowledged, Date :
ICT Administrator	ICT Manager

CONFIDENTIAL DOCUMENT - TO BE FILLED BY ICT ADMINISTRATOR
DO NOT PHOTO-COPY WITHOUT CONSENT FROM HEAD OF INFORMATION DIVISION

LAMPIRAN 16. CATATAN PEMBANGUNAN GANTI APLIKASI

BNPB

Application Development Change

Badan Nasional Penanggulangan Bencana
PUSDATINMAS
Floor 4, Gedung BNPB
Jl. Ir. Hj. Juanda No. 36,Jakarta Pusat, Indonesia
Phone: (021) 3442734, 3442985, 3443079
Facsimile: (021) 3505075

Form No. 02-02 **LOCATION: H.O. JAKARTA**

Application Name	Build	Version	Changes		Recorded by

IT Administrator	IT Manager
Date	Date

CONFIDENTIAL DOCUMENT - TO BE FILLED BY ICT ADMINISTRATOR
DO NOT PHOTO-COPY WITHOUT CONSENT FROM HEAD OF INFORMATION DIVISION

LAMPIRAN 17. KONTROL PERUBAHAN

BNPB

Change Control

Badan Nasional Penanggulangan Bencana
PUSDATINMAS
Floor 4, Gedung BNPB
Jl. Ir. Hj. Juanda No. 36,Jakarta Pusat, Indonesia
Phone: (021) 3442734, 3442985, 3443079
Facsimile: (021) 3505075

LOCATION: H.O. JAKARTA

Form No. 02-02 Change Control No:	STATUS: ❑ New ❑ Update ❑ Migrate
Completed Date :	
Requested by :	Reference Document:

SYSTEM INFORMATION

DESCRIPTION: *(Please specify the system description)*	**ASSET NUMBER:**
DETAIL SPECIFICATION: *(Please specify the detail specification)*	
BRAND/VENDOR NAME: _____ **TYPE/MODEL/SERIES/VERSION:** *(Please specify detail type/model/series/version)*	Serial Number: _____ Part Number: _____ Released year: _____
CATEGORY: *(Please specify system category)* ❑ COMPUTER HARDWARE AND PERIPHERAL'S ❑ COMMUNICATION ❑ SOFTWARE/APPLICATIONS/OPERATING SYSTEMS ❑ SECURITY/ADMIN PASSWORD ACCOUNT ❑ OTHERS _____	**ENVIRONMENT DESCRIPTION:** *(PLEASE SPECIFY FOR MIGRATION//UPGRADE PURPOSES)* ❑ Source (Server name/path/location) _____ ❑ Destination (Server name/path/location) _____
DETAIL EXISTING SYSTEM INFORMATION: *(Please describe existing system information)*	
LICENCE OR CONTRACT AGREEMENT INFORMATION: *(Please specify if available)*	

CONTACT INFORMATION

VENDOR INFORMATION:
_____
_____

Completed By	*Approved By*	*Approved By*	*Acknowledged By*
_____ *System Administrator* *Date :*	_____ *IT Supervisor* *Date :*	_____ *IT Manager* *Date :*	_____ *IT Head* *Date :*

LAMPIRAN 18. CATATAN PENGUNAAN MOBIL KOMUNIKASI

BNPB

Log COMOB Usage

Badan Nasional Penanggulangan Bencana
Pusat Data Informasi dan Humas
Floor 4, Gedung BNPB
Jl. Ir. H. Juanda No. 36 Jakarta Pusat, Indonesia
Phone: (021) 577 2030 (Hunting)
Facsimile: (021) 577 2040 - 43

Completed by COMOB Driver - Please fill in COMOB Status log/checklist before departure and after returning from duty/mission (by other than travelling staff)

Form No. 03-01

LOCATION: H.O. JAKARTA

Day	Date	Time	Car No	Driver No.	Full Name	From	To	Purpose	Total people in car	Departure Status Log Done	Returning Status Log Done	Start Mileage	End Mileage	Refill Amount (litre)

COMOB Driver	IT Supervisor	IT Manager
Date	Date	Date

CONFIDENTIAL DOCUMENT - TO BE FILLED BY COMOB DRIVER - PHOTO-COPY ALLOWED - SUBMIT TO INFORMATION DIVISION AT BNPB PUSDATINMAS

LAMPIRAN 19. DAFTAR INVETARIS STATUS MOBIL KOMUNIKASI

BNPB

COMOB Status Check List

Pusat Data Informasi dan Humas
Floor 4, Gedung BNPB
Jl. Ir. Hj. Juanda No. 36,Jakarta Pusat, Indonesia
Phone: (021) 3442734, 3442985, 3443079 Facsimile: (021) 3505075

LOCATION: H.O. JAKARTA

Form No. 03-02

Diisi oleh staf selain tim KOMOB - Isi sebelum berangkat dan setelah kembali

Tipe checklist (Berangkat or Tiba): [ ]

Tanggal diperiksa (Tgl./Bln./Thn.):	Jam diperiksa (24):
Nomor KOMOB:	Nomor Plat:
Lokasi sekarang:	
Lokasi tujuan (bila berangkat):	
Staff:	Nomor telepon:
Alamat E-Mail:	

Harap ditandai dengan tanda ✓ bila memenuhi syarat atau tanda ✖ bila tidak memenuhi syarat

EKSTERIOR (BAGIAN LUAR)		Satelit VSAT pada tempatnya, kokoh, dan berfungsi	
Tanggal nomor-plat kendaraan bagian depan masih berlaku		Antena HF pada tempatnya, kokoh, dan berfungsi	
Jumlah ban lengkap dan dalam kondisi baik		Antena VHF pada tempat and kokoh atau aman	
Mesin derek depan pada tempatnya, kokoh, dan berfungsi baik		Antena VHF dapat dinaikkan dan berfungsi	
Penahan benturan depan pada tempatnya dan berfungsi baik		**INTERIOR BAGIAN PENGEMUDI**	
Lampu sorot jalan bagian depan lengkap dan berfungsi baik		STNK dan surat kendaraan lain lengkap, pada tempatnya, dan aman	
Lampu sorot bagian atas lengkap dan berfungsi baik		Alat kemudi secara keseluruhan pada kondisi yang baik	
Logo BNPB bagian depan lengkap dan jelas atau mudah dibaca		Minyak untuk perjalanan cukup untuk berangkat dan kembali	
TV himbauan masyarakat merek yang benar dan berfungsi		Sistem radio pengemudi depan pada tempatnya dan berfungsi	
Speaker kiri dan kanan untuk himbauan lengkap dan berfungsi		**INTERIOR BAGIAN OPERATOR**	
Alat mikrofon tersedia dan berfungsi		Semua komputer pada tempatnya, kokoh, dan berfungsi	
Tanggal nomor-plat kendaraan bagian belakang masih berlaku		Semua kursi, meja, dan laci pada tempatnya dan kondisi terawat	
Generator belakang pada tempatnya, kokoh, dan berfungsi		Semua sistem komunikasi radio pada tempatnya dan berfungsi	
Bahan bakar untuk generator tersedia cukup untuk misi atau tugas		Semua sistem komunikasi satelit pada tempatnya dan berfungsi	
Lampu sorot jalan bagian belakang pada tempatnya dan berfungsi		Semua *Power Stabilizer* dan UPS pada tempatnya dan berfungsi	
Lampu sorot belakang bagian atas lengkap dan berfungsi baik		Alat pendingin (AC) ruangan pada tempatnya dan berfungsi	
Penutup bagian kiri untuk melihat operator dapat dibuka		Kaki tanah bisa diturunkan dan berfungsi dengan baik	

Staf Pemeriksa	Pengemudi KOMOB	Manajer ICT	Kepala Bidang Informasi
Tanggal	Tanggal	Tanggal	Tanggal

LAMPIRAN 20. CATATAN MOBIL KOMUNIKASI

BNPB

COMOB Notes

Pusat Data Informasi dan Humas
Floor 4, Gedung BNPB
Jl. Ir. Hj. Juanda No. 36,Jakarta Pusat, Indonesia
Phone: (021) 3442734, 3442985, 3443079, Facsimile: (021) 3505075

Form No: 03-03
LOCATION: H.O. JAKARTA

Completed by COMOB Driver - Report to PUSDALOPS Manager after full or if critical and require immediate action

District:	COMOB No.:	Day:	Date (DMY):	Recorded by:

District:	COMOB No.:	Day:	Date (DMY):	Recorded by:

District:	COMOB No.:	Day:	Date (DMY):	Recorded by:

COMOB Driver Date	ICT Manager Date	Head of Information Division Date

LAMPIRAN 21. DAFTAR PERALATAN PELAYANAN

BNPB

LIST EQUIPMENT SERVICES

Badan Nasional Penanggulangan Bencana
PUSDATINMAS, Floor 4, Gedung BNPB
Jl. Ir. Hj. Juanda No. 36,Jakarta Pusat, Indonesia
Phone: (021) 3442734, 3442985, 3443079
Facsimile: (021) 3505075

Form No. 04-01 Tanggal: **LOCATION: H.O. JAKARTA**

No	No. Tag	Serial Number	Description	Quatity

Status	Recorded by:	Acknowledge by:
☐ ASAP ☐ Schedule ☐ Other	IT Helpdesk	IT Supervisor

LAMPIRAN 22. TENAGA PENDUKUNG TEKNIS

Technical Support Request

Pusat Data Informasi dan Humas
Floor 4, Gedung BNPB
Jl. Ir. Hj. Juanda No. 36,Jakarta Pusat, Indonesia
Phone. (021) 3442734, 3442985, 3443079 Fax:(021) 3505075

LOCATION: H.O. JAKARTA

Form No. 04-02 Incident No. [ ] fixed. [ ]

Date submit (DMY):		Time submit (24):		
Name:	Phone:	E-Mail:		
Department:	Division:	Building:	Floor:	Room:

Do NOT fill in the following row

By Staff:	Date received (DMY):	Time received (24):

Please TICK which technical support you require

HARDWARE	SOFTWARE	NETWORK
[ ] Workstation	[ ] Windows / Drivers	[ ] Internet Connectivity
[ ] Monitor only	[ ] Microsoft Office	[ ] LAN Connectivity
[ ] Keyboard / Mouse only	[ ] Internet Browser	[ ] WiFi / Hotspot
[ ] Office Laptop	[ ] Anti-Virus	[ ] File Sharing
[ ] Personal Laptop	[ ] Website Access	[ ] Download / Upload
[ ] Printing / Scanning	[ ] Application	[ ] Video Conferencing
[ ] UPS	[ ] Video / Photo / Audio	[ ] User Account
[ ] Power Adaptor / Cable	[ ] WinRAR / WinZIP	[ ] Modem
[ ] Optical / External Drive	[ ] Undelete / Unformat	[ ] Satellite / BGAN
[ ] GPS	[ ] Adobe / Scanning	[ ] Phone/Fax/Radio
[ ] Other:	[ ] Other:	[ ] Other:

ICT Administrator Date	ICT Manager Date

PLEASE HAND-IN TO INFORMATION DIVISION AT JUANDA OFFICE
PHOTO-COPY IS ALLOWED - INTERNAL USE ONLY

LAMPIRAN 23. PERANGKAT LUNAK, PERANGKAT KERAS DAN PROSEDUR

BNPB

SOFTWARE, HARDWARE AND PROCEDURE

Badan Nasional Penanggulangan Bencana
Pusat Data Informasi dan Humas
Floor 4, Gedung BNPBJL. Ir. H. Juanda No. 36
Jakarta Pusat. Indonesia
Telp. (021) 3442734, 3442985, 3443079
Fax. (021) 3505075

LOCATION: H.O. JAKARTA

No Form :	**BNPB / BPBD :**
Date :	**Unit / Deputy:**
Requested by :	**Location :**

COMPUTER (check/tick theitem)

- ☐ SERVER
- ☐ NOTEBOOK/LAPTOP
- ☐ DESKTOP
- ☐ LAIN : _____

Computer equipment

- ☐ CPU
- ☐ MONITOR
- ☐ KEYBOARD
- ☐ MOUSE
- ☐ MEMORY
- ☐ PROCESSOR
- ☐ HARDDISK
- ☐ FLASH MODEM
- ☐ CD-ROM
- ☐ PRINTER
- ☐ DATA CABLE
- ☐ POWER CABLE
- ☐ MEDIA DRIVE
- ☐ TAPE BACKUP
- ☐ POWER ADAPTOR
- ☐ OTHER ; _____

COMMUNICATION

- ☐ PHONE HANDSET
- ☐ HAND/SMART PHONE
- ☐ RADIO
- ☐ PHONE EXTENSION
- ☐ FAX MACHINE
- ☐ BATTERY/CHARGER
- ☐ PABX
- ☐ LAIN : _____

SOFTWARE

- ☐ SISTEM OPERASI
- ☐ APLIKASI BENCANA
- ☐ APLIKASI UMUM
- ☐ EMAIL
- ☐ DATA BASE
- ☐ CASE TOOLS
- ☐ LAIN : _____

ACCSES TYPE

- ☐ NEW / MODIFY / DELETE
- ☐ SECURE CLIENT

PROCEDURE

- ☐ PROSEDUR DOKUMENTASI
- ☐ JUKNIS DOKUMENTASI
- ☐ FORM DOKUMENTASI
- ☐ OTHER ; _____

Spesificatioin detail description:

_____

_____ Requestor	_____ Head of requestor

Requestor Only

STATUS : ☐ Accept ☐ Reject ☐ Hold	PRIORITY : ☐ Urgent ☐ Normal	**Received by :** _____ **Date :** _____ *Performed date :* _____ *Dikerjakan oleh :* _____ *Biaya yang timbul :* _____

Information Technology Only

Approved by, _____ **KABID INFORMASI**	Checked by, _____ **WAKIL BIDANG INFORMASI**

Notes :

_____

_____

BNPB 001 /SEP/2013

LAMPIRAN 24. PERMINTAAN MIGRASI APLIKASI

Badan Nasional Penanggulangan Bencana
PUSDATINMAS
Floor 4, Gedung BNPB
Jl. Ir. Hj. Juanda No. 36,Jakarta Pusat, Indonesia
Phone: (021) 3442734, 3442985, 3443079
Facsimile: (021) 3505075

Tanggal: _____ **Ruang Lingkup:** _____

Pindah Program Baru

Log :

Nama Program :_____

Kepentingan :_____

Dari :_____(Test Environment)

Ke :_____(Production Environment)

Menu : _____

Dikerjakan oleh	Diuji oleh	Disetujui oleh User	IT Aplikasi Note 1.
IT Aplikasi Manager Note 2.	System Administrator. Note 3.		

Note 1. Periksa hasil test.
2. Pastikan semua sudah di tanda-tangani oleh pihak terkait.
3. Migrasi ke program baru melalui production system.
4. Prosedur Administrasi semua dokumen kelengkapan log.

LAMPIRAN 25. PERMINTAAN PELATIHAN

BNPB

Training Request

Pusat Data Informasi dan Humas

Floor 4, Gedung BNPB
Jl. Ir. Hj. Juanda No. 36,Jakarta Pusat, Indonesia
Phone: (021) 3442734, 3442985, 3443079, Facsimile: (021) 3505075

Request No. [_____] Delivered [ ]

Form No. 05-01 **LOCATION: H.O. JAKARTA**

Date submit (DMY):		Time submit (24):		
Name:	Phone:	E-Mail:		
Department:	Division:	Building:	Floor:	Room:

Do NOT fill in the following row

By Staff:	Date received (DMY):	Time received (24):

Please TICK which capacity training/mentoring you require

[ ] Basic Microsoft Word	[ ] Update Anti-Virus	[ ] Basic Networking
[ ] Mail Merge	[ ] Create and edit PDF file	[ ] Internet Messengers
[ ] Basic Microsoft Excel	[ ] Compress and extract Files	[ ] Basic Computer Security
[ ] Pivot Table	[ ] Basic GIS	[ ] Audio Video Conference
[ ] Basic Microsoft PowerPoint	[ ] Register and use E-Mail	[ ] Cloud Storage / Backup
[ ] Basic Microsoft Access	[ ] Google Contacts	[ ] Basic Database
[ ] Basic Microsoft Project	[ ] Google Calendar	[ ] Basic System Analyst
[ ] Basic Microsoft Outlook	[ ] E-Mail with BNPB	[ ] Basic Photo Editing
[ ] Basic OpenOffice	[ ] OpenStreetMap	[ ] Basic IT Hardware
[ ] Basic Programming	[ ] Ina-SAFE	[ ] Radio Telecommunication
[ ] Basic MySQL	[ ] DIBI	[ ] Software Troubleshooting
[ ] Other	[ ] Other	[ ] Other

User / Client	IT Manager
Date	Date

PLEASE HAND-IN TO INFORMATION DIVISION AT JUANDA OFFICE
PHOTO-COPY IS ALLOWED - INTERNAL USE ONLY