



**KEMENTERIAN PERTAHANAN RI
PUSAT DATA DAN INFORMASI**

**PEDOMAN KERJA
BUSINESS CONTINUITY MANAGEMENT
PUSDATIN KEMHAN**

Nomor : PK/03/VIII/2022/PUSDATIN

TAHUN 2022

BUSNINESS CONTINUITY PLAN

1. Tujuan

Tujuan utama dari *Business Continuity Plan* (BCP) adalah untuk memungkinkan pimpinan terus mengelola operasi bisnis dalam kondisi yang sulit dengan melakukan *strategy recovery* yang tepat sehingga pemulihan dan kelangsungan bisnis segera berjalan. Hal ini dilakukan dengan mempertimbangan risiko operasional manajemen dan rencana manajemen krisis.

2. Dokumen BCP ini menjelaskan:

- a. Ruang lingkup.
- b. Identifikasi, penilaian risiko, dan kondisi kritis serta mitigasi yang dapat menyebabkan ancaman terhadap keberlangsungan bisnis.
- c. Analisis Dampak Kontinuitas Bisnis (Penghitungan *Maximum Acceptable Downtime*, MTPD (*Maximum Tolerable Period of Disruption*) dan RTO (*Request Time Out*) yaitu suatu kondisi dimana koneksi internet kita pada lalu lintas data terjadi gangguan sehingga muncul informasi pada Command Prompt.
- d. Tugas dan tanggung jawab tim *business continuity*.
- e. Lokasi koordinasi BCP.
- f. Prosedur/petunjuk pelaksanaan ketika terjadi kondisi kritis.
- g. Skenario penanganan kondisi kritis.
- h. Keanggotaan tim *business continuity* dan *call list*.
- i. Sosialisasi BCP.
- j. Pengujian BCP. dan
- k. Lampiran (formulir/ data/ *template* yang diperlukan).

3. Ruang Lingkup

BCP diaktifkan pada saat terjadi kondisi kritis, yaitu terjadinya gangguan bisnis yang serius dan menyebabkan ketidaktersediaan layanan bisnis yang berkepanjangan.

BAB I IDENTIFIKASI DAN PENILAIAN RISIKO KEBERLANGSUNGAN BISNIS

1. Identifikasi dan Penilaian Risiko Keberlangsungan Bisnis

Berikut adalah hasil identifikasi kondisi-kondisi yang berpotensi menciptakan kondisi kritis yang dapat mengganggu keberlangsungan bisnis Pusdatin Kemhan RI.

a. *Risk Assessment.*

NO	Kondisi	Konsekuensi Terparah	Dampak	Tingkat Kemungkinan	Tingkat Keparahan	Kategori Dampak
1	Berada di lingkungan yang mudah tergenang banjir	Terjadinya banjir yang merendam fasilitas instansi dengan ketinggian > 1 meter	a. Terputusnya akses ke kantor b. Rusaknya perangkat IT & perangkat pendukung c. Rusak/ hilangnya dokumen, <i>file</i> , dan <i>database</i> karena kerusakan media penyimpanan d. Terhentinya seluruh/ sebagian kegiatan operasional	1	5	5 (Sedang)
2	Banyak nya ekspatriat yang keluar dan masuk instansi	Terjangkit nya wabah penyakit regional (cth. Covid, SARS, Flu Burung, dsb)	a. Banyak pegawai yang absen/tidak bisa hadir ke kantor b. Diberhentikan nya seluruh kegiatan untuk pencegahan penularan penyakit	1	5	5 (Sedang)

			c. Kekosongan posisi strategis akibat kematian pegawai			
3	Berada di area publik	Gangguan keamanan dari lingkungan sekitar Terjadinya tindakan anarkis	a. Dihentikannya seluruh kegiatan Organisasi demi keselamatan b. Kerusakan perangkat/ dokumen/ <i>file</i> karena tindakan anarkis	1	5	5 (Sedang)
4	Pasokan listrik yang kurang stabil (pada saat bersamaan terdapat kesulitan dalam mendapatkan BBM untuk Genset)	Terputusnya aliran listrik dalam waktu yang lama (di atas kemampuan genset)	a. Berhentinya kegiatan produksi/ sistem IT b. <i>Availability data/file</i> menjadi terganggu	1	5	5 (Sedang)
5	Berada di dekat gunung berapi aktif	Tertimpa material vulkanik yang merusak alat dan kesehatan	a. Banyak pegawai yang absen/tidak bisa hadir ke kantor b. Rusaknya perangkat IT & peralatan produksi. c. Hilangnya/ rusaknya dokumen dan/ atau <i>file</i> akibat material vulkanik	1	5	5 (Sedang)

6	Kawasan yang tidak memiliki sarana pemadam kebakaran	Kebakaran yang terjadi di kawasan/ sekitarnya merembet memasuki kawasan instansi	a. Kerusakan perangkat vital (misalnya <i>server</i> , mesin produksi, dsb) b. Kehilangan/ kerusakan data/ dokumen c. Kekosongan posisi strategis akibat kematian pegawai	1	5	5 (Sedang)
7	Kelalaian yang bersifat fatal	Terjadi ledakan, Kebakaran, korsleting listrik, dsb	a. Kerusakan perangkat vital (misalnya <i>server</i> , data center dan dsb) b. Kehilangan/ kerusakan data/ dokumen c. Kekosongan posisi strategis akibat kematian pegawai	1	5	5 (Sedang)
8	Kelemahan bawaan (defect) yang terdapat pada perangkat vital (cth. <i>server</i> , jaringan internet, dsb)	Kegagalan fungsi peralatan vital	a. Berhentinya fungsi jaringan internet b. Terganggunya /berhentinya layanan IT c. Kehilangan data	1	5	5 (Sedang)
9	Semakin banyak nya serangan <i>hacker</i>	Kegagalan operasional <i>server</i> / sarana komputasi	a. Terganggunya /berhentinya layanan IT b. Kehilangan data.	1	5	5 (Sedang)

10	Gangguan Umum Kamtibmas	Pencurian Perampokan Penculikan/ Penyandera Pemblokiran akses	a. Kehilangan informasi/ data/ dokumen penting b. Kekosongan posisi strategis akibat kematian pegawai	1	5	5 (Sedang)
----	-------------------------	---	--	---	---	------------

Tingkat keparahan didefinisikan sebagai berikut:

NO	<i>Severity (keparahan)</i>	<i>Explanation</i>	<i>Score</i>
1	<i>Insignificant</i>	<i>No impact</i>	0
2	<i>Minor</i>	<i>No extra effort required to repair</i>	1
3	<i>Significant</i>	<i>Tangible harm, extra effort required to repair</i>	2
4	<i>Damaging</i>	<i>Significant expenditure of resources required -- Damage to reputation and confidence</i>	3
5	<i>Serious</i>	<i>Extended outage and / or loss of connectivity -- Compromise of large amounts of data or services</i>	4
6	<i>Grave</i>	<i>Permanent shutdown -- Complete compromise</i>	5

Tingkat kemungkinan didefinisikan sebagai berikut:

NO	<i>Likelihood (kemungkinan)</i>	<i>Explanation</i>	<i>Score</i>
1	<i>Negligible</i>	<i>Unlikely to occur</i>	0
2	<i>Very Low</i>	<i>2 – 3 times every 5 years</i>	1
3	<i>Low</i>	<i>Up to once per year</i>	2
4	<i>Medium</i>	<i>Up to twice a year</i>	3
5	<i>High</i>	<i>Up to once per month</i>	4
6	<i>Very High</i>	<i>More than once per month</i>	5
7	<i>Extreme</i>	<i>Several times a week or day</i>	6

b. Mitigasi Risiko (*Risk Mitigation*)

NO	Kondisi	Konsekuensi Terparah	Mitigasi (Antisipasi dan Penanganan)
1	Berada di lingkungan yang mudah tergenang banjir	Terjadinya banjir yang merendam fasilitas Intansi dengan ketinggian > 1 meter	Mitigasi terhadap keutuhan data/informasi: <i>Backup</i> rutin untuk data-data yang ada pada <i>server</i> Persiapkan Prosedur Kondisi Kritis
2	Banyaknya ekspatriat yang keluar dan masuk Intansi	Terjangkitnya wabah penyakit regional (cth. Covid, SARS, Flu Burung, dsb)	Deteksi suhu tamu (ketika lebih dari 38 derajat C, maka tamu dilarang masuk Penyiapan prosedur penanganan infeksi Covid, SARS, Flu Burung oleh tim HSE dan paramedis Implementasi Sistem Manajemen (ISO) dengan baik, sehingga ketergantungan terhadap personil berkurang Persiapkan prosedur kondisi kritis
3	Berada di area publik	Gangguan keamanan dari lingkungan sekitar	Mitigasi terhadap keutuhan data/informasi: <i>Backup</i> rutin untuk data-data yang ada pada <i>server</i> Pemagaran keliling Patroli keliling Persiapkan prosedur kondisi kritis
4	Pasokan listrik yang kurang stabil (pada saat bersamaan terdapat kesulitan dalam mendapatkan BBM untuk Genset)	Terputusnya aliran listrik dalam waktu yang lama (di atas kemampuan genset)	Menyediakan pemasok BBM genset lebih dari satu Persiapkan Prosedur Kondisi Kritis Pemastian agar UPS <i>server</i> selalu berjalan dengan baik (tanpa <i>error</i>), sehingga apabila listrik terputus masih ada waktu untuk melakukan <i>proper shutdown</i>
5	Berada di dekat Gunung Berapi Aktif	Tertimpa material vulkanik yang merusak (alat dan kesehatan)	Mitigasi terhadap keutuhan data/informasi: <i>Backup</i> rutin untuk data-data yang ada pada <i>server</i> Persiapkan prosedur kondisi kritis
6	Kawasan yang tidak memiliki sarana pemadam kebakaran	Kebakaran yang terjadi di kawasan/ sekitarnya merembet	Mitigasi terhadap keutuhan data/informasi: <i>Backup</i> rutin untuk data-data yang ada pada <i>server</i> Pemastian berkala bahwa APAR dan Hidrant dalam kondisi siap pakai

		memasuki area instansi	Persiapkan prosedur kondisi kritis
7	Kelalaian yang bersifat fatal	Terjadi ledakan, Kebakaran, korsleting listrik, dsb	Penerapan Disiplin Pemeriksaan rutin aspek HSE health, safety, and environment (merupakan rangkaian indentifikasi bahaya di lingkungan kerja Mitigasi terhadap keutuhan data/informasi: <i>Backup</i> rutin untuk data-data yang ada pada <i>server</i> Persiapkan prosedur kondisi kritis
8	Kelemahan bawaan (<i>defect</i>) yang terdapat pada perangkat <i>vital</i> (cth. <i>server</i> , jaringan internet, dsb)	Kegagalan fungsi peralatan <i>vital</i>	Mitigasi terhadap keutuhan data/informasi: <i>Backup</i> rutin untuk data-data yang ada pada <i>server</i> Berlakukan prosedur pengujian perangkat dan pengecekan penerimaan barang Persiapkan prosedur kondisi kritis
9	Banyaknya serangan <i>hacker</i>	Kegagalan operasional <i>server</i> /sarana komputasi	Mitigasi terhadap keutuhan data/informasi: <i>Backup</i> rutin untuk data-data yang ada pada <i>server</i> Penerapan SMKI Penerapan Prosedur <i>Vulnerability Assesment</i> dan <i>Penetration Testing</i> Penerapan Prosedur <i>Insident Handling</i> Persiapkan prosedur kondisi kritis
10	Gangguan Umum Kamtibmas	Pencurian Perampokan Penculikan/ Penyanderaan	Pemagaran keliling Pemasangan Sistem Monitoring Pengamanan Markas Patroli Keamanan Persiapkan prosedur kondisi kritis

BAB II ANALISIS DAMPAK TERHADAP KONSINTINUITAS

2. Analisis Dampak Terhadap *Kontinuitas*

a. Perhitungan Maximum Acceptable Downtime

Maximum Acceptable Downtime ditentukan oleh manajemen berdasarkan kerugian (dalam rupiah) yang dapat ditanggung oleh Pusdatin Kemhan RI.

Catatan: Berikut adalah layanan-layanan IT yang diidentifikasi sebagai non kritis terhadap Pusdatin Kemhan RI (untuk Kekritisan Dampak < 55%) dan tidak akan tersedia selama kondisi kritis:

- 1) *Layanan Active Directory.*
- 2) *Layanan Antivirus.*
- 3) *Layanan File dan Pencetakan.*
- 4) *Layanan Enkripsi Laptop dan Hard Disk.*
- 5) *Layanan Sistem Payroll.*
- 6) *Layanan PC/Laptop.*
- 7) *Tim Aplikasi Bisnis.*
- 8) *Sistem Internet.*
- 9) *Sistem Switching, dan*
- 10) *Sistem Firewall.*
 - a) *Maximum Acceptable Downtime* untuk berhentinya kegiatan total operasional dan ketersediaan data di Pusdatin Kemhan RI adalah 2 hari.
 - b) *Maximum Acceptable Downtime* untuk berhentinya kegiatan operasional Pusdatin Kemhan RI (namun kegiatan penyediaan data ke Pihak pengguna layanan masih dapat dilakukan) adalah 4 hari.
 - c) *Maximum Acceptable Downtime* untuk terputusnya akses ke Pusdatin Kemhan RI adalah 2 hari.
 - d) *Maximum Acceptable Downtime* untuk ketidakhadiran salah satu posisi kunci di Pusdatin Kemhan RI adalah 20 hari (kepala sub bidang ke atas).

b. Perhitungan *Maximum Tolerable Period of Disruption* (MTPD)

MTPD adalah sebuah nilai dalam satuan waktu yang mengindikasikan berapa lama Pusdatin Kemhan RI mampu kehilangan sebuah proses bisnis. Perhitungan MTPD didasarkan dari *best practice* dan analisis downtime perangkat dan/atau maksimum pendapatan yang hilang akibat terhentinya operasional Pusdatin Kemhan RI, yang mampu ditanggung oleh Pusdatin Kemhan RI.

MTPD Infrastruktur IT = 7 hari

MTPD untuk Seluruh Kegiatan Pusdatin Kemhan RI + Penyediaan Data = 4 hari

MTPD Untuk seluruh kegiatan Operasional Pusdatin Kemhan RI = 5 hari

MTPD untuk akses ke Pusdatin Kemhan RI = 4 hari

MTPD untuk ketidakhadiran satu posisi kunci di Pusdatin Kemhan RI = 20 hari

c. *Recovery Point Objective* (RPO) / Sasaran Point Pemulihan

Recovery Point Objective (RPO) adalah jumlah hari maksimum yang diperlukan untuk menangani downtime. RPO berdasarkan *best practice* dan analisa tidak boleh melebihi MTPD. Hal ini adalah *objective* pemulihan aktifitas ketika terjadi kondisi kritis.

RPO Infrastruktur IT = 6 hari.

RPO untuk Seluruh Kegiatan Operasional Pusdatin Kemhan RI + Penyediaan Data = 3,5 hari

RPO Untuk seluruh kegiatan Operasional = 4 hari

RPO untuk akses ke Pusdatin Kemhan RI = 3,5 hari

RPO untuk ketidakhadiran satu posisi kunci di Pusdatin Kemhan RI = 19 hari

BAB III TUGAS DAN TANGGUNG JAWAB TIM BCM

3. Tugas dan Tanggung Jawab Tim BCM

Bagian ini memberikan gambaran tanggung jawab fungsional masing-masing tim pemulihan. Tiga tim akan dikerahkan untuk menanggapi bencana, yaitu:

- a. Tim Manajemen Krisis (*Crisis Management Team*).
- b. BCM Koordinator dan Wakil Koordinator BCM, Dan
- c. Tim Pemulihan IT.

1) Tim Manajemen Krisis (TMK)

- a) TMK bertanggung jawab untuk memberikan arahan secara keseluruhan operasi pemulihan. Tim ini memberikan informasi tingkat kerusakan, mengaktifkan organisasi pemulihan dan mengarahkan upaya pemulihan serta upaya restorasi fasilitas yang rusak.
- b) TMK juga bertindak sebagai kontak utama untuk memberikan status update ke para pemangku jabatan yang berwenang dalam Pusdatin Kemhan RI. Pusdatin Kemhan RI akan bertanggung jawab untuk komunikasi dan hubungan ke media, jika diperlukan. dan
- c) TMK bertanggung jawab untuk memutuskan perlu atau tidaknya dilakukan prosedur pemulihan bencana. Jika diputuskan bahwa hal itu perlu dilakukan, maka prosedur ini mulai dijalankan oleh organisasi/TMK selama bencana itu terjadi, dan bekerja sama dengan struktur manajemen saat ini.

2) Koordinator BCM dan Wakil Koordinator BCM

- a) Koordinator BCM adalah anggota dari Tim Manajemen Krisis sedangkan Wakil Koordinator BCM merupakan bagian dari Tim Pemulihan TI saat bencana.
- b) Koordinator BCM/Wakil Koordinator BCM bertanggung jawab untuk menilai kerusakan dan menyatakan tingkat keparahan bencana dan tingkat respon yang diperlukan untuk bertahan dan pulih.
- c) Koordinator BCM/Wakil Koordinator BCM bertanggung jawab untuk membantu dan mengkoordinasikan dalam pelaksanaan respons dan strategi operasi alternatif saat bencana. dan
- d) Koordinator BCM/Wakil Koordinator BCM bertanggung jawab untuk berkomunikasi dengan afiliasi instansi selama bencana.

3) Tim Pemulihan IT

- a) Tim Perbaikan TI bertanggung jawab atas pengadaan dan instalasi peralatan komputer dan komunikasi.
- b) Tim Perbaikan TI bertanggung jawab untuk memulihkan pemrosesan komputer dan menjalankan kelangsungan

kegiatan bisnis, sesuai dengan jadwal pemulihan untuk kondisi sistem yang kritis.

- c) Tim Perbaikan TI bekerja sama dengan tim lain terkait untuk mengembalikan kondisi sistem yang sesuai keadaan sebelumnya dengan dukungan sistem aplikasi bisnis. dan
- d) Tim Perbaikan TI bertanggung jawab untuk memastikan link jaringan yang dibutuhkan tersedia di lokasi yang aman.

BAB IV PUSAT PUSAT KOORIDINASI DALAM KONDISI KRITIS

4. Pusat-Pusat Koordinasi Dalam Kondisi Kritis

a. Titik-Titik Evakuasi

Berikut ini menunjukkan titik lokasi pertemuan (01 s/d 09 ditunjukkan sebagai lingkaran merah) ketika terjadi kondisi kritis yang memerlukan evakuasi bagi staf di lokasi.

b. Pusat Komando Alternatif (*Alternate Command Centre Site*)

Berikut ini menunjukkan lokasi pusat komando ketika terjadi kondisi kritis yang menyebabkan seluruh staf harus dievakuasi dari Pusdatin Kemhan RI atau seluruh staf tidak dapat mencapai lokasi Pusdatin Kemhan RI:

Site	Pusdatin Kemhan RI
Address	
Contact Number	
Alternate Number 1	
Alternate Number 2	

Apabila *alternate command centre site* di atas tidak dapat difungsikan, maka alternatif lainnya adalah:

Site	Pusdatin Kemhan RI
Address	
Contact Number	
Alternate Number 1	
Alternate Number 2	

Ini adalah *checklist* dari fasilitas (misalnya saluran telepon), peralatan (PC misalnya), dan catatan penting (misalnya formulir,

log) yang perlu tersedia untuk melanjutkan operasi di pusat komando selama krisis. *Checklist* harus ditinjau sebagai bagian dari latihan tinjauan tahunan, seperti dibawah ini.

Sumber daya	Qty	Disediakan oleh
Telepon	1	
White Board	1	
Komputer dengan Printer	1	
Mesin fax	1	
Meja tulis + kursi	1	
Stationery - White Board Marker, buku tulis, pena, Pensil	1 Set	

BAB V

PROSEDUR/PETUNJUK PELAKSANAAN KETIKA TERJADI KONDISI KRITIS

5. Prosedur/Petunjuk Pelaksanaan Ketika Terjadi Kondisi Kritis

- a. Prosedur Penanganan Respon Awal terhadap Terjadinya Kondisi Krisis.

Proses respon terhadap krisis ini digunakan ketika seorang pelapor menginformasikan Pusdatin Kemhan RI tentang terjadinya keadaan yang mengarah kepada kondisi kritis. Jika potensi krisis terdeteksi (dilaporkan oleh pegawai/pihak yang berwenang di luar instansi), maka dilakukan urutan langkah berikut:

- 1) Penerima laporan meneruskan laporan tersebut kepada tim TMK, dan
- 2) Tim TMK mengadakan rapat singkat (dapat menggunakan *conference call/telepon/SMS/email*) untuk memutuskan apakah sudah masuk kondisi kritis atau belum (ketika hal ini dilakukan, didefinisikan sebagai T0).
- 3) Jika diputuskan bahwa kondisi kritis sudah terjadi, maka:
 - a) Tim TMK melakukan *assessment* terhadap dampak yang terjadi dengan maksimum waktu yang dibutuhkan untuk ini adalah 30 menit (waktu yang diperlukan untuk kegiatan ini dinamakan dengan T1).

- b) Ketua Tim TMK mengumumkan keadaan kritis dan Prosedur Kondisi Kritis dilaksanakan (ketika hal ini dilakukan, didefinisikan sebagai T2).
 - c) Tim Keamanan mengkoordinasikan pengamanan lapangan.
 - d) Tim Evakuasi menentukan apakah perlu dilakukan evakuasi. Jika iya, maka jalankan prosedur mobilisasi dan Ketua Tim TMK mengkoordinasikan pengaktifan Pusat Koordinasi Alternatif (*Alternate Command Centre Site*).
 - e) Tim HSE menyiapkan prosedur dan peralatan P3K, dan
 - f) Tim IT melakukan evaluasi apakah diperlukan *shutdown system* IT. Jika iya, dilakukan prosedur *shutdown* IT.
- b. Prosedur Relokasi Pusat Komando

Persiapan Relokasi Pusat Komando adalah sebagai berikut:

 - 1) Manajemen menyiapkan tempat dan kelengkapan Pusat Komando.
 - 2) Penguatan tim, dan
 - 3) Menginformasikan lokasi bencana serta arahan lokasi alternatif.
- c. Prosedur untuk Pemberian Pernyataan Pers
 - 1) Ketua TMK akan menjadi sumber utama komunikasi dengan pihak eksternal selama kondisi kritis berlangsung. Dan
 - 2) Tidak ada karyawan lain selain Ketua TMK yang memiliki kewenangan untuk berkomunikasi dengan pihak eksternal termasuk media atau pers berkenaan dengan setiap aspek kejadian.
- d. Prosedur Mobilisasi Sumber Daya
 - 1) Rapat koordinasi awal

Agenda ini dapat digunakan sebagai panduan (sebagian atau keseluruhan) bagi Ketua Tim Manajemen Krisis untuk melakukan pertemuan ketika diputuskan dilakukan mobilisasi sumber daya termasuk tim pemulihan IT. Seorang sekretaris dapat ditunjuk sebelum pertemuan untuk mencatat hasil keputusan.

- 2) Penilaian dampak mobilisasi terhadap layanan, peralatan, dan personil Hal ini perlu dilakukan untuk menilai tingkat kerugian terhadap mobilisasi, seperti:
 - a) Apa saja layanan peralatan yang terkena secara total/sebagian (lihat daftar layanan dampak yang disiapkan oleh Tim Pemulihan IT)?.
 - b) Dapatkah layanan/peralatan dioperasikan diluar dari tempat yang ada?. Dan
 - c) Adakah korban jiwa Bagaimana cara penanganan terhadap korban?.
- 3) Kegiatan mobilisasi sumber daya.
Untuk memobilisasi seluruh anggota tim pemulihan dan mengidentifikasi sumber daya non-lokal IT lain yang dibutuhkan. Tentukan sumber-sumber lain yang diperlukan untuk pemulihan, untuk diingatkan atau dimobilisasi dari:
 - a) *Extended* sumber daya IT.
 - b) *Vendor*.
 - c) Lokasi yang ditunjuk, dan
 - d) *Business Group*.
- 4) Menginformasikan mobilisasi operasional instansi ke instansi lainnya.

Untuk memastikan bahwa Operasional instansi ke instansi lainnya diinformasikan dengan segera dan benar serta upaya pemulihanya.
 - a) Kapan harus menginformasikan?
 - b) Siapa yang akan menginfomasikan?
 - c) Apa yang diinformasikan?
 - d) Frekuensi status *update* berikutnya?
 - e) Siapa yang menyetujui rilis informasi dan ditujukan kepada siapa, misalnya Ketua Tim *Helpdesk* menyetujui semua komunikasi untuk menjalankan instansi, Ketua

Tim Manajemen Krisis menyetujui komunikasi ke kantor lain.

- 5) Menyepakati tujuan masing-masing tim untuk 3 jam berikutnya Untuk memastikan bahwa semua tim mengetahui segera langkah selanjutnya dan dapat melanjutkan untuk melakukan tugas-tugas segera setelah pertemuan ini.
- 6) Penentuan status *update* dan frekuensi rapat
Untuk memastikan bahwa anggota tim menyadari waktu laporan status, terutama pertemuan berikutnya setelah pertemuan mobilisasi pertama :
 - a) Berapa kali pertemuan berikutnya?
 - b) Apa pedoman umum untuk frekuensi laporan status jika pertemuan tidak dimungkinkan?
 - c) Kepada siapa tim pemulihan akan melapor?

BAB VI

BEBERAPA SKENARIO PENANGANAN KONDISI KRITIS

6. Beberapa Skenario Penanganan Kondisi Kritis

a. Skenario Tipe 1

Terjadi Kebakaran Banjir	
Skenario Kondisional	
Terjadi banjir kiriman secara tiba-tiba sekitar pukul, dengan genangan air di lantai dasar kantor hingga naik mencapai meter dalam jam, dan terus bertambah. Atas dasar hal tersebut, maka perlu dilakukan evakuasi terhadap pegawai, mematikan seluruh listrik serta pemindahan <i>server</i> ke tempat <i>alternative</i>	
Objektivitas Pemulihan Waktu (Berdasarkan scenario terburuk)	
T2 + 20 jam	
Persiapan Sebelum Krisis	
Null	
Prosedur Kondisi Darurat	
Target Selesai	Aktifitas
T0	Atas dasar laporan yang masuk, tim TMK melakukan rapat untuk menentukan status kondisi darurat
T1	TIM TMK melakukan analisis dampak bencana.

T2	TIM TMK memerintahkan evakuasi menyeluruh, perangkat IT inti
T2+0,5 jam	Petugas memastikan listrik dimatikan
T2+1 jam	Tim evakuasi mengkoordinasikan evakuasi sehingga seluruh pegawai di instansi berkumpul di titik-titik evakuasi atau tempat-tempat yang lebih tinggi, yang berada di area/sekitar area instansi
T2+3 jam	Tim evakuasi mengkoordinasikan evakuasi ke luar area
T2+3 jam	Tim TMK mengkoordinasikan pengaktifan <i>alternate site command</i>
T2+1 jam	Tim IT melakukan <i>proper shutdown procedure</i> terhadap semua <i>server</i> yang ada di <i>data center</i>
T2+5 jam	Tim IT mengkoordinasikan evakuasi <i>main server</i> ke <i>alternate site command</i>
T2+7 jam	Tim TMK berusaha mencapai <i>alternate site command</i>
T2+12 jam	Ketika <i>alternate site command</i> sudah diaktifkan, maka ketua/wakil ketua tim TMK harus melakukan hal-hal sebagai berikut : - Melakukan pengecekan status karyawan secara berantai dari atasan ke masing-masing bawahannya, sesuai dengan hirarki organisasi - Memberitahukan kepada seluruh pihak terkait (pihak pengguna layanan, media, dsb) tentang kondisi terakhir operasional instansi. - Menetapkan kegiatan minimum yang harus dilakukan (misalnya: komunikasi, koordinasi, penyelamatan aset-aset penting, pendataan korban, dsb)
T2+20 jam	
N/A	Setiap hari tim TMK berkoordinasi pada <i>alternate command site</i> untuk mengkoordinasikan kegiatan-kegiatan minimum yang harus dilakukan, termasuk penentuan akhir dari kondisi krisis.
Prosedur Kembali ke Normal	
Tim Infrastruktur IT harus melakukan analisa akar penyebab untuk mencegah insiden serupa terjadi lagi	
Keterangan	
N/A	

b. Skenario Tipe 2

Terjadinya Wabah Penyakit Menular (cth. Covid-19, Flu Babi, SARS, Flu Burung)	
Skenario Kondisional	
Pada tanggal terdapat setidaknya orang menderita demam. Setelah itu – atas koordinasi tim paramedis - dilakukan pemeriksaan oleh petugas dari klinik terdekat. jam kemudian, berdasarkan hasil test darah, dilaporkan bahwa setidaknya karyawan Pusdatin Kemhan RI sudah positif terkena wabah Covid-19, sehingga diputuskan untuk dilakukan evakuasi termasuk <i>data center</i> harus dipindahkan ke lokasi <i>alternative</i>	
Objektivitas Pemulihan Waktu (Berdasarkan scenario terburuk)	
T2 + 30 jam	
Persiapan / Permintaan Perlengkapan selama Pra-Krisis	
1. Termometer x 1 2. N95 masker	
Prosedur Kondisi Darurat	
Target Selesai	Aktifitas
T0	Atas dasar laporan yang masuk, tim TMK melakukan rapat untuk menentukan status kondisi darurat
T1	TIM TMK melakukan analisis dampak bencana
T2	TIM TMK memerintahkan prosedur karantina, dimana tidak ada pegawai yang boleh keluar atau masuk selama karantina diberlakukan, tanpa seijin petugas
T2+0,5 jam	Petugas mengkoordinasikan evakuasi orang yang sudah dikonfirmasi terjangkit virus Covid-19 tersebut ke rumah sakit terdekat
T2+4 jam	Petugas mengkoordinasikan pembagian <i>masker</i> serta cuci tangan menggunakan sabun <i>antiseptic</i>
T2+3 jam	Petugas mengkoordinasikan untuk dihadirkan tim <i>paramedic</i> dari rumah sakit terdekat, yang memiliki kemampuan untuk menangani wabah Covid-19
T2+15 jam	Petugas berkoordinasi dengan tim <i>paramedic</i> terdekat, melakukan pemeriksaan darah terhadap semua pegawai dan memisahkan para pegawai yang sudah terinfeksi dan yang belum terinfeksi
T2+24 jam	Petugas mengkoordinasikan evakuasi seluruh karyawan yang belum terinfeksi ke luar area
T2+24 jam	Petugas mengkoordinasikan evakuasi seluruh karyawan yang telah terinfeksi ke rumah sakit-rumah sakit terdekat
T2+30 jam	Petugas mengkoordinasikan disinfektan terhadap seluruh infrastruktur

T2+30	TIM TMK mengaktifkan <i>alternate site command</i> dan menentukan kegiatan operasional minimum yang harus tetap dilakukan selama kondisi krisis, termasuk ketentuan pengakhiran masa krisis
Prosedur Kembali ke Normal	
Memulihkan semua layanan lainnya	
Penjelasan	

c. Skenario Tipe 3

Lumpuhnya Jaringan Komputer	
Skenario Kondisional	
Pada tanggal puluhan orang dari setiap bagian yang ada di instansi, memberikan laporan kepada bagian IT Infrastruktur bahwa mereka tidak dapat mengakses <i>share folder</i> , melakukan <i>printing</i> dan mengirim <i>email</i>	
Objektivitas Pemulihan Waktu (Berdasarkan skenario terburuk)	
T2 + 4,5 jam	

Prosedur Kondisi Kritis	
Target Selesai	Aktifitas
T0	Bagian IT Infrastruktur mengkomunikasikan kepada tim TMK
T1	Tim TMK terkait (bagian IT) melakukan <i>assessment</i> terhadap dampak
T2	Tim Pemulihan IT mengusahakan <i>troubleshooting</i> IT serta menghubungi vendor terkait untuk memberikan bantuan terhadap <i>troubleshooting</i> (cth. mengganti <i>core switch</i> , dsb)
T2+4 jam	Setelah pemulihan jaringan berhasil, maka Bagian IT Infrastruktur mengkomunikasikan status terakhirnya kepada tim TMK
T2+4,5 jam	Tim TMK menginformasikan secara hirarki organisasi kepada semua bagian/bidang bahwa jaringan telah kembali normal
Prosedur Kembali ke Normal	
Tim Infrastruktur IT harus melakukan analisa akar penyebab masalah untuk mencegah insiden serupa terjadi lagi	
Keterangan	

d. Skenario Tipe 4

Terputusnya Aliran Listrik	
Skenario Kondisional	
Pada tanggal listrik dari PLN setempat padam. Pemadaman terjadi pada area yang cukup luas, dan <i>area-area</i> lain di Kota Hal ini menyebabkan kelangkaan solar sehingga petugas kesulitan untuk menjaga genset agar tetap hidup. Pada hari kedua pukul seluruh aliran listrik di instansi padam	
Objektivitas Pemulihan Waktu (Berdasarkan skenario terburuk)	
T ₂ (24 hours) + 12 hours = 36 hours	
Persiapan Sebelum Krisis	
N/A	
Prosedur Kondisi Kritis	
Target Selesai	Aktifitas
1	Atas dasar laporan yang masuk, tim TMK melakukan rapat untuk menentukan status kondisi darurat
2	TIM TMK melakukan analisis dampak bencana.
3	TIM TMK memerintahkan evakuasi menyeluruh, perangkat IT inti.
4	Tim IT melakukan <i>proper shutdown procedure</i> terhadap semua <i>server</i> yang ada di <i>data center</i>
5	Tim IT melakukan evakuasi <i>main server</i>
6	Tim IT mengkoordinasikan evakuasi <i>main server</i> ke <i>alternate site command</i>
7	Tim TMK berusaha mencapai <i>alternate site command</i>
8	Ketika <i>alternate site command</i> sudah diaktifkan, maka ketua/wakil ketua tim TMK harus melakukan hal-hal sebagai berikut: - Memberitahukan kepada seluruh pihak terkait (pihak pengguna layanan, media, dsb.) tentang kondisi terakhir operasional instansi - Menetapkan kegiatan minimum yang harus dilakukan (misalnya: komunikasi, koordinasi, penyelamatan aset-aset penting, pendataan korban, dsb) - Tim Pemulihan IT berusaha menghidupkan <i>main server</i> dan mengkoneksikan ke jaringan yang terdapat di <i>alternate site command</i>
Prosedur Kembali ke Normal	
BCM Koordinator, Wakil Koordinator BCM & tim IT - Infra harus melakukan analisis akar penyebab untuk mencegah insiden serupa terjadi lagi	
Remarks	
N/A	

BAB VII
KEANGGOTAAN TIM BUSINESS CONTINUITY DAN CALL LIST

7. Keanggotaan Tim *Business Continuity* dan *Call List*

a. TMK (Tim Manajemen Krisis)

Tim Manajemen Krisis		
Nama	Penunjukan	Nomor telepon

b. Tim Pemulihan IT

Tim Pemulihan IT - Semua layanan jaringan (Ketua Tim)		
Nama	Penunjukan	Nomor telepon

Tim Pemulihan IT - Keamanan Informasi (Ketua Tim)		
Nama	Penunjukan	Nomor telepon

Tim Pemulihan TI - sistem perkuatan tim (Ketua Tim)		
Nama	Penunjukan	Nomor telepon

c. *Critical Vendors Call List*

Nama Vendor	Kontak Personal	Nomor Telepon	Personal Alternatif	Nomor Telepon	Keterangan
Pemadam Kebakaran					
Polisi (Polsek)					
RS					
Badan SAR Nasional					

Koordinator Kawasan Industri					
Ketua RT Setempat					
Ketua RW Setempat					
Posko Bencana Kelurahan Setempat					
PLN					
Telkom					
Pemasok Solar u/ Genset –					
Server – PT.					
Server – PT.					
Network – PT.					
Internet – PT.					

BAB VIII SOSIALISASI BCP

8. Sosialisasi BCP

- a. BCP harus disosialisasikan pada seluruh pegawai.
- b. Dokumen BCP ini harus tersedia pada seluruh bagian/bidang instansi serta harus tersedia di *site-site* yang telah ditunjuk sebagai *alternate site command*. dan
- c. Setiap ada perubahan, maka dokumen BCP ini harus disosialisasikan kembali.

BAB IX PENGUJIAN BCP

9. Pengujian BCP

Untuk menilai tingkat kesiapan terhadap penanganan kondisi kritis, maka BCP harus dilakukan pengujian sebagai berikut:

- a. Setiap tahun harus dilakukan “*table top test*” (pengujian kesiapan tim terhadap beberapa skenario melalui diskusi). *Table top test* ini dipimpin oleh salah seorang anggota TMK.
- b. Setiap tiga tahun harus dilakukan pengujian dengan cara simulasi
- c. Setiap setelah pengujian dan/atau terjadi kondisi krisis, keefektifan BCP harus dievaluasi.

Hasil pengujian dan/atau evaluasi BCP harus didokumentasikan.

BAB X LAMPIRAN

10. Lampiran

- a. Daftar Pemberitahuan Mitra Kerja
Jika terjadi hal-hal krisis, Wakil Koordinator BCM akan mengirim *email* ke alamat berikut untuk memberitahu mereka tentang krisis yang terjadi.

<i>Group Email</i>	Deskripsi

- b. Formulir Laporan Status BCP untuk Status Laporan : Respon Segera

Laporan Ini harus dilaporkan kepada Koordinator Organisasi BCM di Pusat Komando. Mohon membuat laporan dengan format contoh sebagai berikut:

Dilaporkan Oleh:	
Bagian/Bidang: BAGIAN TATA USAHA	Tanggal:

No. Telepon:	Waktu:
1 Evakuasi dari gedung kantor (Aktivasi pada jam Kantor)	
2 Struktur panggilan Bagian/Bidang (Aktivasi dari luar kantor) (Mohon cantumkan nama-nama staf yang tidak dapat dihubungi)	
3 Aktivasi awal prosedur pemulihan	
4 Jika ada permasalahan lain. Mohon diinformasikan jika anda memerlukan bantuan dari Pusat komando	

c. *Checklist* Penilaian Kerusakan

Checklist ini harus dilaporkan kepada Koordinator Organisasi BCM di Pusat Komando. Mohon isi laporan berikut:

Dilaporkan Oleh:					
Bagian/Bidang: Manajemen Krisis				Tanggal:	
No. Telepon:				Waktu:	
Deskripsi Kerusakan					
Fasilitas		Tandai Jika Terdapat Kerusakan	Penilaian Kerusakan		
Wilayah yang Terkena					
<i>Air Conditioner</i>					
Jaringan					
Lain - lain					
S/ N	Lokasi	Fungsi	Unit Pendukung Fungsi Bisnis	Tandai Jika Rusak	Keterangan
1					
2					
3					
4					
5					
6					
7					

d. Status Laporan : Kelanjutan & Pemulihan

Laporan ini dilaporkan kepada Koordinator Organisasi BCM di Pusat Komando. Mohon isi contoh *form* laporan sebagai berikut:

Dilaporkan Oleh:	
Bagian/Bidang: Pamsis/Banglola/Infratik/TU	Tanggal:
No. Telepon:	Waktu:
1 Apa masalah yang dihadapi selama beroperasi di lokasi alternatif?	
2 Apa masalah yang dihadapi dalam hubungan eksternal, misalnya dengan pihak ketiga atau vendor ?	
3 Jika ada permasalahan lain. Mohon beritahu jika anda memerlukan bantuan dari Pusat komando	

e. Status Laporan : Perbaikan

Laporan ini dilaporkan kepada Koordinator Organisasi BCM di Pusat Komando. Mohon isi contoh *form* laporan sebagai berikut:

Dilaporkan Oleh:	
Bagian/Bidang: IT	Tanggal:
No. Telepon:	Waktu:
1 Apa masalah yang dihadapi ketika kembali ke lokasi utama?	
2 Apa ada permasalahan lain ? Mohon beritahu jika anda memerlukan bantuan dari Pusat komando.	

f. Daftar Data yang Dilakukan *Backup* Harian

Jenis <i>Backup</i> : <i>Backup</i> Harian Database Pusdatin Kemhan RI		
Pemilik :		
Lokasi : Kantor Pusdatin Kemhan RI dan		
Cara Ambil : Jalankan <i>Schedule Backup</i> harian dan simpan di <i>Tera Harddisk</i> Seminggu 1 kali setiap hari Selasa kirim <i>CD backup</i> ke		
<i>Labels Reference</i>		

g. Pernyataan Media

---- Untuk Dirilis Segera ----

Selamat siang bapak – bapak dan ibu – ibu dan terimakasih atas kedatangannya.

Saya (Nama), juru bicara yang ditunjuk untuk Pusdatin Kemhan RI. Pusdatin Kemhan RI telah terkena dampak (peristiwa) terhadap bisnis kami. Kami ingin meyakinkan kepada karyawan kami, keluarga mereka, pemasok dan *stakeholder* bahwa kami telah mempersiapkan sebelumnya untuk peristiwa semacam ini. Kami telah mengembangkan, mengajari dan melatih tim pemulihan kami sebagai langkah proaktif demi kelangsungan operasi bisnis kami. Prioritas utama kami adalah keselamatan karyawan dan anggota keluarga mereka.

Kami telah mengaktifkan rencana *Business Continuity and Emergency Operations* kami, dan persiapan tanggap darurat kami sedang dalam proses. Saat ini kami sedang melakukan komunikasi yang erat dengan *supplier, vendor* dan pemerintah daerah saat ini.

Saya anggota dari Tim *Emergency Operations Center* (EOC) dan saya perlu kembali ke EOC sebagai bagian dari pekerjaan saya. Pusdatin Kemhan RI kami berkomitmen untuk melakukan komunikasi rutin yang efektif dan itu adalah peran saya sebagai anggota tim ini. Pada saat ini saya tidak memiliki informasi yang dapat disampaikan. Saya akan melakukan briefing rutin setiap jam di (lokasi penunjukan).

Saya ingin memberitahu anda, sebagai bagian dari prosedur Operasi Darurat, kami telah meningkatkan tindakan keamanan kami. Oleh karena itu, mohon rencanakan saat kedatangan anda kepada staf

keamanan kami yang nanti akan memvalidasi tanda pengenalan anda dan akses proses anda. Terima kasih atas pengertian Anda

Jika akan melakukan briefing tambahan Anda akan segera diberitahu

Opsional:

Saya punya waktu hanya untuk 1 atau 2 pertanyaan saja. sekarang saya tidak memiliki informasi khusus.

BAB XI PENUTUP

11. Penutup

- a. Demikian Pedoman Business Continuity Management ini di buat, sebagai acuan dalam pengamanan informasi di Pusdatin.
- b. Pedoman ini berlaku sejak di tandatangani dan ketentuan yang belum tercantum dalam pedoman ini akan diatur lebih lanjut dengan memperhatikan perkembangan Sistem Manajemen Keamanan Informasi.
- c. Dokumen asli dari prosedur ini dipelihara dan dikendalikan oleh Dokumen Kontrol di Bidang Pamsisinforan Pusdatin Kemhan RI.
- d. Penggunaan Dokumen asli ataupun dokumen salinan harus mengikuti aturan yang tertulis pada Dokumen Prosedur Pengendalian Dokumen Nomor: SOP/22/VIII/2022/PUSDATIN.

Dikeluarkan di Jakarta
Pada tanggal Agustus 2022

Kepala Pusat Data dan Informasi,

Rionardo
Brigadir Jenderal TNI