LAMPIRAN I
PERATURAN MENTERI LUAR NEGERI
REPUBLIK INDONESIA
NOMOR 8 TAHUN 2019
TENTANG
PENGAMANAN KEMENTERIAN LUAR NEGERI DAN PERWAKILAN REPUBLIK INDONESIA

PENGELOLAAN RISIKO KEAMANAN

Komite Pengamanan dan Tim Pengamanan melakukan pengelolaan risiko keamanan di wilayah masing-masing sesuai tahapan sebagai berikut:

1. Penetapan Risiko Keamanan

Risiko Keamanan dikelola dalam batas waktu tertentu, yaitu paling sedikit dalam 1 (satu) tahun.

Kriteria yang digunakan untuk melakukan penetapan risiko keamanan fisik atau keamanan personel atau keamanan informasi yang dikelola risiko keamanannya oleh Tim Pengamanan mencakup:

a. Tingkat frekuensi/kemungkinan terjadinya risiko keamanan

	Kemungkinan	**Deskripsi**	**Skala Nilai**
(1)	**(2)**	**(3)**	**(4)**
1.	1 (Sangat jarang)	Kemungkinan terjadi > 1 tahun ke depan	1
2.	2 (Jarang)	Mungkin terjadi sekali dalam 1 tahun	2
3.	3 (Cukup sering)	Mungkin terjadi sekali dalam 1 bulan	3
4.	4 (Sering)	Mungkin terjadi lebih dari dua kali dalam 1 bulan	4
5.	5 (Sangat sering)	Mungkin terjadi lebih dari lima kali dalam sebulan	5

b. Tingkat dampak risiko;

Tabel 1: Tingkat Risiko Keamanan Personel

Tingkat	Dampak
1 (sangat rendah)	Tidak menimbulkan gangguan atau luka terhadap personel perwakilan
2 (rendah)	Tidak menyebabkan luka fisik, namun menimbulkan gangguan psikologis
3 (sedang)	Menyebabkan luka ringan, atau menimbulkan kondisi yang memerlukan perawatan khusus
4 (tinggi)	Menyebabkan luka berat terhadap beberapa personel sekaligus, dapat menimbulkan kondisi kritis
5 (sangat tinggi)	Berpotensi menyebabkan hilangnya nyawa dan atau menimbulkan cacat fisik permanen

Tabel 2: Tingkat Risiko Keamanan Fisik

Tingkat	Dampak
1 (sangat rendah)	Tidak berpengaruh langsung terhadap keamanan pelaksanaan operasional
2 (rendah)	Ada ancaman yang nyata terhadap keamanan, tetapi belum mengganggu pelaksanaan operasional
3 (sedang)	Terganggunya pelaksanaan operasional
4 (tinggi)	• Terhambatnya penyelenggaraan Negara, pelayanan publik, sumber daya nasional dan/atau ketertiban umum • Terhambatnya perlindungan dan pengamanan infrastruktur strategis
5 (sangat tinggi)	Membahayakan kedaulatan Negara, keutuhan wilayah Negara kesatuan Republik Indonesia dan/atau keselamatan bangsa

Tabel 3: Tingkat Risiko Keamanan Informasi

Tingkat	Dampak
1 (sangat rendah)	Tidak merugikan apapun
2 (rendah)	Mempersulit pelaksanaan tugas
3 (sedang)	Terganggunya kinerja dan fungsi Kementerian Luar Negeri
4 (tinggi)	• Terganggunya fungsi penyelenggaraan Negara, pelayanan publik, sumber daya

	nasional dan/atau ketertiban umum • Terganggunya posisi daya tawar dan strategi yang akan dan telah diambil oleh Negara dalam hubungan dengan negosiasi internasional • Terganggunya perlindungan dan pengamanan infrastruktur strategis Indonesia di Luar Negeri
5 (sangat tinggi)	Dapat membahayakan kedaulatan Negara, keutuhan wilayah Negara kesatuan Republik Indonesia dan/atau keselamatan bangsa

Catatan: Tingkatan dampak risiko keamanan informasi yang apabila informasi tersebut rusak/tidak utuh, diakses oleh pihak yang tidak berhak, atau tidak dapat diakses mempunyai tingkatan yang berbeda.

c. Tingkat status risiko

0 – 5 = Risiko Rendah		**Tingkat Dampak**				
6 – 10 = Risiko sedang		Sangat rendah **1**	Rendah **2**	Sedang **3**	Tinggi **4**	Sangat Tinggi **5**
11 – 15 = Risiko Tinggi						
16 – 25 = Risiko Ekstrim						
Skala Kemungkinan Terjadi	Sangat sering **5**	5	10	15	20	25
	Sering **4**	4	8	12	16	20
	Cukup sering **3**	3	6	9	12	15
	Jarang **2**	2	4	6	8	10
	Sangat jarang **1**	1	2	3	4	5

2. Identifikasi risiko kejadian/kerawanan;

a. Tahap Identifikasi risiko kejadian dilakukan untuk mengidentifikasi kejadian-kejadian yang dapat mengancam dan mengganggu keamanan personel, tamu kementerian dan perwakilan, aset fisik, dan informasi di Kementerian dan Perwakilan.

b. Sumber data dan informasi yang dapat dirujuk untuk menentukan identifikasi risiko kejadian yaitu:
   1) statistik tindak kriminal dari polisi lokal;
   2) pengendalian laporan insiden ancaman dan gangguan yang dikumpulkan oleh Kementerian atau Perwakilan;
   3) data demografi/kondisi sosial resmi yang menyediakan informasi mengenai kondisi ekonomi, kerapatan populasi, jumlah populasi manusia, tingkat pengangguran, dan lain-lain;
   4) informasi intelijen;

5) media massa;
6) faktor lingkungan seperti: suhu, akses lokasi kerja, potensi bencana alam, dan bencana karena manusia;
7) laporan terakhir pelaksanaan bimbingan teknis dan evaluasi sistem pengamanan di Kementerian atau Perwakilan;
8) laporan pengaduan masyarakat;
9) standar operasional prosedur pengamanan Kementerian dan Perwakilan;

c. Identifikasi risiko keamanan dilakukan oleh Komite Pengamanan dan Tim Pengamanan.

d. Identifikasi risiko keamanan dilakukan dengan cara mengidentifikasi apa, mengapa, bagaimana, dan kapan ancaman dan gangguan keamanan aset fisik, personel, tamu dan informasi terjadi atau berulang terjadi pada lingkungan Kementerian atau Perwakilan.

e. Kejadian yang mungkin terjadi/mungkin dapat berulang terjadi diidentifikasi sebanyak mungkin dan dibuat untuk setiap objek pengamanan.

3. Analisis risiko keamanan;

Analisis risiko keamanan adalah aktivitas menentukan tingkat kemungkinan/frekuensi suatu risiko keamanan dan tingkat dampak suatu risiko dengan memperhatikan penanganan risiko yang sudah dilakukan, dan diakhiri dengan menentukan tingkat risiko.

Langkah-langkah Analisis Risiko Keamanan dilakukan dengan:
a. mengidentifikasi aset yang ingin dilindungi dan mengelompokannya dari segi ancaman yang dihadapi:berupa ancaman aset fisik, ancaman personel, ancaman terhadap tamu atau ancaman informasi;

b. mengidentifikasi penyebab dan dampak negatif risiko. Penyebab risiko yang diidentifikasi sebisa mungkin adalah penyebab utama yang dapat bersumber dari internal organisasi (*man, money, material, method, facility/machinery*), atau eksternal organisasi seperti kondisi perekonomian, politik, sosial, teknologi, dan peraturan perundangan;

c. mendokumentasikan penanganan yang sudah dilakukan yang dapat berupa salah satu atau gabungan penanganan/penguatan dari segi *people/process/facility*; dan

d. mendokumentasikan kejadian-kejadian yang diidentifikasi tersebut ke dalam bentuk pernyataan risiko dan ke dalam formulir Register Risiko Keamanan sebagaimana contoh berikut:

Contoh Register Risiko Keamanan

No.	Aset Yang Ingin Dilindungi	Penyebab Internal atau eksternal (1)	Penanganan yang sudah ada *(people/ process/ facility)* (2)	Sisa Risiko (3)	Kemungkinan/ Frekuensi Kejadian (4)	Dampak (5)	Tingkat Risiko (6) (Perkalian antara 3 dan 4)	Status Risiko (7)
Risiko: Ancaman Keamanan Fisik								
1	Premis Perwakilan	Serangan Bersenjata	Pagar ganda, Bunker	Tidak adanya keamanan internal bersenjata lengkap				
2	Premis Perwakilan	*Trespassing*	Pemasangan CCTV	Hanya terdapat 1 orang pengamanan mandiri				
3	Premis Perwakilan	Bom/Ledakan	Pagar ganda, Keamanan internal bersenjata lengkap	Bunker	–			
4	BMN	Kebakaran	Pemasangan alat pencegah kebakaran *(water sprinkler, smoke detector)*	Tidak terdapat POS Pencegahan kebakaran				
Risiko: Ancaman Keamanan Personel								
1	VIP/Keppri	Instabilitas Politik	Rencana kontijensi	Tidak adanya keamanan internal bersenjata lengkap				
2	Staf Perwakilan	Perampokan terhadap individu	POS menghadapi situasi perampokan	Staf belum pernah mendapatkan pelatihan menghadapi situasi berbahaya				
3	Staf Perwakilan	Penculikan	POS menghadapi situasi penculikan	Belum adanya alat komunikasi yang tersambung langsung dengan Keamanan Perwakilan				
4	Pegawai Setempat	Penggalangan	Pembinaan pegawai secara kontinyu	Belum pernah dilakukan pencegahan kegiatan intelijen asing melalui pemindaian elektronik (Sterilisasi)				
5	VIP/Keppri	Pengiriman Paket/Benda Asing/Surat Kaleng	Membuat POS penerimaan barang kiriman	Tidak terdapat mesin X-ray				
6	Staf Konsuler	Ancaman Telepon	*Voice recorder* pada alat komunikasi	Tidak terdapat POS antisipasi ancaman verbal				
Risiko: Ancaman Keamanan Informasi								
1	Data pribadi dalam komputer	*Malware*	Memastikan setiap perangkat komputer dilengkapi	Perwakilan belum memiliki *firewall*				

			dengan anti virus yang *up to date*					
2	Data dalam Server	*Social Engineering*	POS penerimaan tamu dan POS penggunaan *visitor's card*	Perwakilan belum menerapkan kebijakan tamu meninggalkan semua alat elektronik di pos pengamanan				
3	Informasi sensitif negara	Penyadapan	Menggunakaan *jammer* saat membicaraan informasi yang bersifat rahasia (seperti di ruang rapat)	Masih menggunakan telefon genggam biasa untuk komunikasi dengan pimpinan di Pusat				
4	Data dalam komputer	*Hacker*	Memasang alat pengamanan jaringan sistem teknologi informasi (*firewall*)	Belum dilakukan pembagian pembagian topologi jaringan				

4. Evaluasi Risiko Keamanan

   a. evaluasi Risiko Keamanan adalah kegiatan membandingkan tingkat risiko yang diperkirakan dengan kriteria tingkat risiko yang sudah ditetapkan. Evaluasi Risiko menghasilkan daftar urut tingkat risiko keamanan yang dapat digunakan untuk mengidentifikasi skala prioritas risiko keamanan yang harus dikelola.

   b. Tahap ini dimaksudkan untuk menyediakan daftar skala prioritas risiko dari yang paling memerlukan penanganan hingga yang paling tidak memerlukan penanganan sehubungan dengan keterbatasan sumber daya yang dimiliki untuk menangani risiko.

   c. Skala prioritas risiko terdiri dari risiko tinggi, risiko sedang, dan risiko rendah.

   d. Keluaran dari tahap identifikasi risiko keamanan, analisis risiko keamanan, dan evaluasi risiko keamanan adalah Register Risiko Keamanan per Kementerian Luar Negeri atau masing-masing Perwakilan sebagaimana disusun oleh masing-masing Tim Pengamanan (lihat contoh tabel pada butir 3 di atas).

5. Penanganan Risiko Keamanan

   a. Penanganan risiko keamanan adalah aktivitas-aktivitas yang ditujukan untuk menghilangkan penyebab risiko atau mengurangi tingkat kemungkinan terjadinya risiko atau meminimalkan dampak/konsekuensi terhadap keamanan aset fisik, personel, tamu dan informasi.

   b. Risiko yang rendah atau dapat diterima harus dipantau dan ditelaah secara periodik untuk menjamin bahwa risiko tersebut tetap dapat

diterima. Jika risiko tidak masuk dalam kategori risiko rendah atau risiko yang dapat diterima, maka risiko tersebut harus ditangani dengan menggunakan satu atau lebih opsi penanganan risiko, yang dapat mencakup:

1) Peningkatan kapasitas dan kesadaran personel terhadap pengamanan;
2) Peningkatan sarana dan prasarana pengamanan;
3) Pembuatan/pemutakhiran Standar Operasional Prosedur;
4) Permintaan kunjungan tim terpadu Bimbingan Teknis dan Evaluasi Pengamanan Kementerian dan Perwakilan yang dikoordinir oleh Sekretaris Komite Pengamanan; dan
5) Permintaan bantuan pengamanan.

c. Tahapan penanganan risiko:

1) Tim Pengamanan merancang cara/langkah penanganan respon risiko dengan mengembangkan berbagai opsi penanganan atau respon risiko.
2) Penanganan atau respon risiko dapat berupa upaya menghindari risiko (tidak melakukan kegiatan yang menimbulkan risiko), mengurangi kemungkinan terjadinya risiko (misal perbaikan SOP), dan mengurangi dampak risiko (misal klarifikasi di media massa atas dampak reputasi yang sudah terjadi). Penentuan cara/langkah penanganan atau respon risiko memperhatikan cara/langkah penanganan risiko yang selama ini sudah dilakukan (tidak sekedar mengulang) dan sebisa mungkin menghilangkan penyebab utama risiko.
3) Tim Pengamanan dapat meminta bimbingan teknis dari Sekretariat Komite Pengamanan dalam rangka memilih cara/langkah penanganan risiko yang terbaik yang diyakini mampu menghilangkan atau mengurangi penyebab utama terjadinya risiko dan menggunakan pertimbangan biaya dibanding manfaat yang akan diperoleh. Cara/langkah penanganan atau respon risiko dapat lebih dari satu untuk setiap risiko. Alokasi sumber daya untuk respon risiko diprioritaskan sesuai dengan tingkat risiko dimulai dari risiko tinggi, sedang hingga rendah. Satu hal yang harus dihindari dalam merancang cara/langkah penanganan risiko adalah mencantumkan cara/langkah penanganan risiko dengan rumusan yang tidak konkret atau bersifat normatif.
4) Tim Pengamanan dapat bersama-sama dengan Sekretariat Komite Pengamanan merencanakan penanganan risiko keamanan antara lain dengan menentukan pihak yang bertanggung jawab melakukan penanganan, jadwal waktu penanganan, indikator kinerja keberhasilan penanganan, dan perencanaan anggaran yang dibutuhkan untuk penanganan risiko.

5) Tim Pengamanan dapat bersama-sama dengan Sekretariat Komite Pengamanan mengusulkan anggaran biaya penanganan risiko sesuai dengan ketentuan.
6) Output perumusan rencana pengamanan risiko adalah dokumen rencana pengamanan risiko untuk Kementerian atau Perwakilan.

6. Monitoring dan Reviu Risiko Keamanan

a. Monitoring dan reviu adalah aktivitas memantau dan menelaah kinerja pengamanan dan perubahan-perubahan yang mungkin mempengaruhinya dan terutama atas kinerja penanganan risiko.

b. Ruang lingkup monitoring dan reviu adalah perkembangan dan hambatan pelaksanaan penanganan risiko, relevansi risiko, relevansi penyebab, relevansi dampak, relevansi tingkat kemungkinan/frekuensi, relevansi tingkat dampak, dan relevansi penanganan risiko. Monitoring dan Reviu dilakukan secara berkala setiap tiga bulan dan sepanjang waktu penerapan manajemen risiko.

c. Monitoring dan reviu dilakukan dengan tahapan sebagai berikut:
1) Komite Pengamanan dan/atau Tim Pengamanan memonitor perkembangan dan faktor penghambat penanganan risiko yang dilakukan oleh pihak yang bertanggung jawab terhadap penanganan risiko dengan mengacu pada rencana penanganan risiko. Hasil monitoring dan evaluasi menjadi bahan penyusunan laporan pelaksanaan penanganan risiko.
2) Sekretariat Komite Pengamanan memonitor pelaksanaan penanganan risiko keamanan yang dilakukan oleh Tim Pengamanan dengan mengacu pada rencana penanganan risiko dan mereviu relevansi risiko, relevansi penyebab risiko, relevansi skala prioritas risiko, dan relevansi penanganan risiko.
3) Sekretariat Komite Pengamanan dapat menggunakan aplikasi Sistem Informasi Manajemen Pengamanan Perwakilan (SIMPAM) dan/atau forum penyusunan RKA-KL dengan Perwakilan untuk memonitor dan mereviu tindak lanjut penanganan risiko keamanan yang dilakukan oleh Tim Pengamanan pada Perwakilan.
4) Perwakilan dapat mengusulkan kegiatan pengecekan langsung/reviu kepada Sekretariat Komite Pengamanan di wilayah kerja Perwakilan.
5) Usulan pengecekan langsung/reviu dapat berdasarkan permintaan Perwakilan, sesuai RKP dan/atau disposisi Pimpinan Kementerian, analisis awal risiko keamanan Perwakilan, dan/atau pertimbangan rawan dan/atau berbahaya sesuai ketentuan Peraturan Perundang-undangan.
6) Apabila diperlukan suatu perencanaan penanganan risiko keamanan yang memerlukan proses pengadaan yang tidak dapat menggunakan anggaran Perwakilan pada tahun berjalan, jadwal

pengecekan langsung/reviu dapat disesuaikan agar terlaksana sebelum penyusunan RKA-KL tahun berikutnya (antara bulan Februari sampai dengan bulan April).

7) Sekretariat Komite Pengamanan akan mereviu efektivitas penerapan manajemen risiko terutama pada level kebijakan.
8) Data yang digunakan dalam tahap ini adalah rencana penanganan risiko, laporan pelaksanaan penanganan risiko dan bukti-bukti (indikator Output) yang menunjukkan adanya penanganan risiko.
9) Output dari tahapan ini adalah laporan monitoring dan reviu pelaksanaan penanganan risiko. Formulir laporan monitoring pelaksanaan penanganan risiko keamanan dapat dilihat pada contoh di bawah.
10) Reviu Sistem Pengamanan dilakukan oleh Sekretariat Komite Pengamanan, paling sedikit 1 (satu) kali dalam setahun.

Contoh Formulir Laporan Monitoring Pelaksanaan Penanganan Risiko Keamanan

No	Risiko	Rencana Penanganan				Kesesuaian Pelaksanaan terhadap Rencana				Saran
		Uraian	Jadwal	PIC	Anggaran	Menurut Tim Pengamanan/ Perwakilan		Menurut Sekretariat Komite Manajemen Risiko Keamanan		
						Sesuai/ Tidak Sesuai	Hambatan	Sesuai/ Tidak Sesuai	Hambatan	
1										
2										

MENTERI LUAR NEGERI
REPUBLIK INDONESIA,

ttd.

RETNO L.P. MARSUDI

LAMPIRAN II

PERATURAN MENTERI LUAR NEGERI

REPUBLIK INDONESIA

NOMOR 8 TAHUN 2019

TENTANG

PENGAMANAN KEMENTERIAN LUAR NEGERI DAN PERWAKILAN REPUBLIK INDONESIA

PEDOMAN PELAKSANAAN PENGAMANAN

I. STANDAR OPERASIONAL PROSEDUR (SOP) PELAKSANAAN KEGIATAN PENGAMANAN ASET FISIK, PERSONEL, DAN INFORMASI

Kementerian dan Perwakilan perlu menyusun, menetapkan, dan melaksanakan SOP Pengamanan Aset Fisik, tamu, Personel dan Informasi sesuai dengan penilaian terhadap risiko ancaman dan gangguan keamanan yang dihadapi.

SOP Pengamanan Kementerian dan Perwakilan mencakup tanggung jawab masing-masing personel dalam upaya pengamanan.

A. STANDAR OPERASIONAL PROSEDUR PENGAMANAN ASET FISIK

SOP Pengamanan Aset Fisik adalah terkait tanggap darurat atas rangkaian peristiwa yang mengancam dan mengganggu keamanan dan kenyamanan yang disebabkan baik oleh faktor alam dan/atau faktor non-alam maupun faktor manusia sehingga mengakibatkan timbulnya korban jiwa, kerusakan lingkungan, kerugian harta benda, dan dampak psikologis. Situasi darurat dapat bersumber dari dalam atau lingkungan sekitar, antara lain:

a. Kebakaran/ledakan berupa kobaran api yang membesar yang tidak terkendali dan merugikan manusia, barang dan lingkungan baik dari tempat bekerja maupun lingkungan sekitar/penduduk.
b. Huru-hara merupakan situasi atau kondisi yang tidak terkendali tidak diinginkan, menimbulkan kepanikan, kekhawatiran dan mengakibatkan aktivitas kerja terhenti.
c. Ancaman bom yang menyebabkan terjadinya gangguan terhadap aktivitas kerja sehari-hari, normal atau kompleks, dan harus dianggap serius.
d. Bencana alam, seperti gempa bumi, badai siklon, tsunami, dan sebagainya.

1. Aksi Unjuk Rasa

Aksi unjuk rasa damai dapat berkembang menjadi unjuk rasa dengan tingkat ancaman yang tinggi dan menimbulkan kerusakan terhadap infrastruktur Kementerian atau Perwakilan. Pada beberapa kasus, target aksi unjuk rasa bukanlah gedung Kementerian atau gedung Perwakilan. Namun karena gedung Kementerian dan gedung Perwakilan tersebut berada di lokasi yang rawan ancaman kelompok tertentu, memungkinkan terkena dampak negatif.

Untuk mengurangi kemungkinan kerusakan atau kerugian dari kegiatan unjuk rasa perlu diambil langkah sebagai berikut:

1) SOP Aksi unjuk rasa

a. Setiap personel yang mendengar atau menerima informasi adanya rencana unjuk rasa oleh massa yang direncakanan mengarah ke kantor Kementerian atau Perwakilan segera melapor kepada Komite Pengamanan dan/atau Tim Pengamanan.
b. Komite Pengamanan dan/atau Tim Pengamanan memutuskan rencana tindakan/langkah-langkah pencegahan dan penanganan terkait keselamatan lingkungan dalam serta mekanisme pengamanan.
c. Petugas jaga segera mengunci pintu gerbang dan meminta bantuan aparat keamanan setempat untuk meningkatkan pengamanan di luar pagar. Selama aksi unjuk rasa berlangsung, mengamati keadaan di luar gerbang dari tempat yang memungkinkan dan aman;
d. Komite Pengamanan dan/atau Tim Pengamanan memberikan arahan kepada semua personel dan jika perlu menunjuk pejabat yang ditugaskan untuk menerima dan berdialog dengan wakil para pengunjuk rasa;
e. Selama aksi unjuk rasa berlangsung:
   (1) Tidak membuka pintu gerbang utama kecuali atas perintah Komite Pengamanan dan/atau Tim Pengamanan;
   (2) Meminta seluruh tamu yang berada di dalam gedung tetap ditempatnya atau meninggalkan gedung melalui jalur aman;
   (3) Menginstruksikan staf yang berada di luar gedung untuk tidak mendekati gedung namun tetap siaga menunggu instruksi lebih lanjut;
   (4) Menghentikan pelayanan publik hingga aksi unjuk rasa selesai;
   (5) Menginstruksikan semua staf agar menjaga ketenangan dan menghindari tindakan atau ucapan provokatif.

f. Komite Pengamanan dan/atau Tim Pengamanan melakukan koordinasi dengan aparat keamanan setempat.
g. Memantau dan mewaspadai kemungkinan situasi memburuk.
h. Komite Pengamanan dan/atau Tim Pengamanan dapat memberikan mandat kepada pejabat yang ditunjuk untuk meredakan ketegangan dan menampung aspirasi pengunjuk rasa.
i. Dalam keadaan yang terkendali, personel lainnya tetap bersikap tenang dan bekerja seperti biasa.

2) Aksi unjuk rasa anarkis/huru-hara

a. Apabila situasi menjurus pada tindakan anarkis atau kekerasan, maka diambil langkah-langkah sebagai berikut:
   (1) Komite Pengamanan dan/atau Tim Pengamanan segera berkoordinasi lebih lanjut dengan aparat keamanan setempat;
   (2) Komite Pengamanan dan/atau Tim Pengamanan memberikan informasi dan petunjuk langkah Pengamanan kepada semua personel;
   (3) Semua personel mengamankan dokumen-dokumen penting dan barang berharga lainnya;
   (4) Menentukan ruang yang dinilai memadai dan aman untuk dijadikan tempat berkumpul untuk Personel dan tamu;
   (5) Mengoordinasikan Personel Kementerian atau Perwakilan untuk segera berkumpul di tempat yang telah ditentukan;
   (6) Apabila keadaan memburuk di negara tempat premis Kementerian atau Perwakilan berada, premis Kementerian atau Perwakilan dapat dijadikan sebagai tempat berkumpul Personel bersama keluarga masing-masing;
   (7) Petugas jaga yang berada di luar terus memantau keadaan dan secara teratur menyampaikan laporan kepada Komite Pengamanan dan/atau Tim Pengamanan;
   (8) Jika situasi keamanan sudah tidak dapat dikendalikan lagi dan mengancam keselamatan Aset Fisik serta jiwa Personel, Komite Pengamanan dan/atau Tim Pengamanan memimpin upaya evakuasi dan tindakan penyelamatan serta senantiasa berkoordinasi dengan aparat keamanan di luar Kementerian atau Perwakilan.
b. Apabila aksi unjuk rasa telah selesai, semua Personel kembali ke tempat tugas masing-masing.

c. Komite Pengamanan dan/atau Tim Pengamanan dapat menyiapkan laporan khusus mengenai aksi unjuk rasa kepada Menteri.

2. Bencana Alam

Bencana alam dapat menimbulkan berbagai dampak seperti kerusakan terhadap sarana dan prasarana Kementerian atau Perwakilan, berhentinya pelayanan publik, hingga korban jiwa. Untuk itu, Kementerian atau Perwakilan harus menyiapkan berbagai langkah penanganan bencana alam, sebagai berikut:

a. Bencana badai atau angin topan:
   1) segera menutup pintu dan jendela ruangan masing-masing guna menghindari hempasan angin yang dapat menyebabkan kerusakan;
   2) jangan bepergian ke luar gedung pada saat terjadi badai atau angin topan;
   3) personel menghubungi keluarganya agar tetap berada di rumah atau dalam bangunan yang aman;
   4) menyiapkan alat-alat bantu penerangan (lampu senter, lilin, atau lampu penerangan darurat lainnya) untuk menghadapi kemungkinan listrik padam;
   5) jika menggunakan lilin, pastikan lilin tersebut aman dari bahaya kebakaran;
   6) waspada terhadap kemungkinan adanya upaya-upaya pencurian, perampokan serta tindakan kriminal lainnya; dan
   7) setiap Personel menyiapkan persediaan 9 (sembilan) bahan pokok untuk keadaan darurat, minimal cukup untuk 3 (tiga) hari.

b. Bencana gempa bumi:

   1) mencari tempat paling aman dari reruntuhan atau goncangan;
   2) melindungi badan dan kepala menggunakan perlindungan tambahan;
   3) mencari perlindungan di sudut ruangan yang kosong jika tidak terdapat meja atau kursi, atau di sebelah benda-benda kokoh, serta melindungi muka dan kepala dengan tangan;
   4) menghindari langit-langit yang mungkin runtuh, benda-benda yang tergantung di dinding, dan kaca jendela yang mungkin pecah;
   5) menetap di dalam gedung sampai gempa berhenti. Jika harus keluar dari gedung, hati-hati dalam memilih jalan

keluar (mungkin ada tangga yang mengalami kerusakan), usahakan jangan panik dan berlarian;

6) tidak menggunakan lift;
7) apabila sedang berada atau terjebak di dalam lift:
   a) menekan semua tombol dan ketika lift berhenti dan terbuka, segera keluar;
   b) menghubungi pihak lain jika tersedia interphone;
   c) tidak panik dan menghemat penggunaan udara atau oksigen.
   d) memukul pintu lift dengan kencang untuk menarik perhatian.
8) Setelah gempa berakhir:
   a) tetap tenang dan mempersiapkan diri untuk kemungkinan gempa susulan;
   b) tidak menyalakan api, rokok, atau lampu, dan menggunakan alat penerangan;
   c) jika masih di dalam gedung, keluar dengan hati-hati, mewaspadai pecahan kaca atau gelas;
   d) mematikan listrik dan gas;
   e) memeriksa apakah ada orang yang terperangkap dan terluka. Jika ada, segera lakukan pertolongan pertama; dan
   f) menghubungi petugas medis setempat apabila ada yang terluka parah, jangan memindahkan orang yang terluka parah kecuali terdapat kondisi bahaya lanjutan.

c. Bencana tsunami:

Fase persiapan

1) Mempelajari jalur evakuasi tsunami.
2) Mempersiapkan peralatan untuk keadaan darurat yang mudah dibawa dalam 1 (satu) tas yang paling sedikit berisi:
   a) salinan identitas atau dokumen pribadi;
   b) uang atau alat pembayaran lainnya;
   c) air dan makanan instan;
   d) lampu senter;
   e) perlengkapan pertolongan pertama; dan
   f) alat komunikasi.

Fase kejadian

Mengikuti rencana evakuasi yang telah dipersiapkan, menghindari tiang listrik roboh akibat gempa, menghindari bangunan atau jembatan yang runtuh, menjauhi pantai dan mencari tempat yang tinggi (misalnya dataran tinggi atau naik ke bangunan sampai lantai paling atas atau atap).

Fase paska kejadian

Menetap di tempat yang tinggi hingga datangnya pertolongan atau instruksi keadaan darurat dari otoritas setempat yang berwenang.

3. Terorisme

Apabila terdapat ancaman dan gangguan keamanan yang disebabkan oleh terorisme, Kementerian atau Perwakilan melakukan langkah-langkah sebagai berikut:

a. Mencegah Aksi Teror

a) Melaporkan kepada aparat keamanan setempat apabila menemukan benda-benda yang mencurigakan;
b) Memeriksa setiap kendaraan yang masuk ke dalam lingkungan gedung Kementerian atau Perwakilan;
c) Melakukan pemeriksaan terhadap barang bawaan para tamu atau pihak ketiga yang akan masuk ke gedung Kementerian atau Perwakilan;
d) Memastikan CCTV yang menghadap lingkungan luar premis Kementerian atau Perwakilan selalu aktif.
e) Menetapkan prioritas pengawasan terhadap tempat-tempat rawan atau mengandung celah keamanan dengan melaksanakan pengawasan selama maupun sesudah jam kerja oleh petugas jaga atau piket;
f) Jika mendapat ancaman bom melalui telepon:
    a) mencoba mendapatkan informasi sebanyak mungkin dengan cara menanyakan hal-hal sebagai berikut:
        1) Kapan bom akan meledak?
        2) Dimanakah posisi bom?
        3) Seperti apa bentuk/rupa bom?
        4) Apa alat pemicu bom tersebut?
        5) Apakah anda yang meletakkan bom itu?
    b) jika telepon yang digunakan memiliki kemampuan merekam, rekam pembicaraan. Jika tidak, catat percakapan;
    c) menghubungi aparat keamanan dan Komite Pengamanan atau Tim Pengamanan;
    d) mengamankan diri dengan menutup semua akses ruangan hingga memperoleh instruksi lanjutan dari pihak keamanan; dan
    e) melakukan evakuasi dari gedung dan menjauhi tempat berbahaya.
g) Jika terjadi ledakan bom:
    a) menghubungi dan berkoordinasi segera dengan aparat keamanan setempat;

b) bersembunyi di bawah meja atau tempat aman lainnya untuk menghindari tertimpa reruntuhan;
c) meninggalkan gedung dengan tetap waspada terhadap lantai atau tangga yang hancur serta reruntuhan;
d) merangkak atau merayap di lantai jika terdapat asap yang pekat;
e) menghindari tempat atau ruangan yang terbakar;
f) tidak menggunakan lift;
g) menghindari jendela, pintu kaca atau tempat berpotensi bahaya lainnya; dan
h) menggunakan jalur yang telah ditetapkan sebagai jalur evakuasi.

b. Teror Melalui Paket atau Surat

Dalam menghadapi teror melalui Paket atau Surat berbahaya, Kementerian dan Perwakilan melakukan langkah-langkah sebagai berikut:

1) Mengenali Surat atau Paket Berbahaya dengan ciri sebagai berikut:
   a) Nama pengirim tidak dikenal atau tidak jelas;
   b) Nama penerima tidak dikenal, salah pengejaan, tidak lengkap;
   c) Paket atau Surat tidak dialamatkan secara spesifik atau tidak ada nama pengirim dan penerima;
   d) Ditandai dengan tulisan "Pribadi" atau "Rahasia" atau "Jangan masuk *x-ray*";
   e) Terlihat ada kabel atau pelapis aluminium, mengeluarkan bau yang aneh, atau terdapat noda yang tidak dikenal (contoh: bubuk berwarna);
   f) Dibungkus secara berlebihan atau tidak rapih;
   g) Alamat cap pos tidak sama dengan alamat pengirim; dan/atau
   h) Terdengar bunyi yang berdetak secara teratur.

2) Langkah penanganan paket atau surat mencurigakan:
   a) Tidak membuka paket atau surat, mengguncangnya, menunjukannya kepada orang lain, atau mengosongkannya;
   b) Membiarkannya pada tempat ditemukan atau meletakannya pada permukaan yang rata;
   c) Menutupi paket atau surat tersebut dengan benda yang bisa dijadikan sebagai penutup seperti tempat sampah yang telah dikosongkan, baju, atau kain;
   d) Mematikan peralatan elektronik seperti kipas angin atau pendingin udara yang dapat menyirkulasikan lebih

lanjut zat yang terkandung dalam paket atau surat tersebut;

e) Menyiapkan tempat khusus untuk menyortir surat atau paket, terutama yang ditujukan kepada Pejabat Kementerian atau Perwakilan;
f) Menginformasikan kepada orang lain yang berada dekat dengan paket atau surat tersebut agar menjauhkan diri ke tempat aman;
g) Membawa semua barang-barang pribadi guna mengantisipasi tindakan sterilisasi oleh aparat keamanan;
h) Menutup pintu ruangan dimana paket atau surat tersebut berada, menutupi celah-celah pintu tersebut dengan kain, dan memastikan tidak ada orang yang mendekat;
i) Melaporkan kepada aparat keamanan setempat; dan
j) Mencuci tangan secara menyeluruh dengan sabun dan air bersih guna mencegah terpaparnya bagian wajah dengan zat berbahaya.

4. Aksi Sabotase Gedung

Aksi sabotase gedung dapat dilakukan dengan cara meletakkan alat penyadap, perangkat berbahaya, merusak sistem teknologi informasi dan jaringan, dan sebagainya.

Upaya pencegahan terhadap aksi sabotase gedung antara lain:

a. Memastikan bahwa pintu-pintu, pagar, pintu gerbang, lampu penerangan, CCTV, dan alarm bekerja dengan semestinya;
b. Menetapkan prioritas pengawasan terhadap tempat-tempat rawan yang mungkin menjadi sasaran sabotase dengan melaksanakan pengawasan selama maupun sesudah jam kerja oleh petugas jaga/piket;
c. Menempatkan kamera CCTV pada tempat-tempat strategis;
d. Menetapkan tata cara memasuki gedung Kementerian dan Perwakilan yang berlaku bagi personel dan tamu;
e. Mewaspadai tamu, pekerja, atau pihak ketiga yang sedang berada di lingkungan Kementerian dan Perwakilan;
f. Melaporkan hal-hal yang mencurigakan kepada Komite Pengamanan dan/atau Tim Pengamanan;
g. Memeriksa barang-barang yang dibawa para tamu ke dalam Kementerian dan Perwakilan;
h. Meminta tamu untuk menitipkan telepon genggam dan barang bawaannya di *deposit box*;
i. Mengklasifikasi zona di lingkungan Kementerian atau Perwakilan menjadi daerah terbatas dan tertutup; dan
j. Menetapkan pengaturan penjagaan dan pengawasannya sesuai klasifikasi zona.

5. Tindakan vandalisme

Langkah-langkah penanganan tindakan vandalisme sebagai berikut:

a. melakukan koordinasi dengan aparat keamanan setempat jika menemukan aksi vandalisme di lingkungan milik Kementerian atau Perwakilan;
b. mengumpulkan barang bukti aksi vandalisme, dapat berupa foto atau rekaman CCTV untuk dikoordinasikan dengan aparat keamanan setempat;
c. menggunakan *portable all band jammer* untuk mencegah pihak yang melakukan tindakan vandalisme mengunggah tindakannya secara daring.

B. STANDAR OPERASIONAL PROSEDUR PENANGANAN BENCANA KEBAKARAN

1. Pencegahan Kebakaran

Kementerian atau Perwakilan melakukan langkah-langkah pencegahan kebakaran sebagai berikut:

a. menyusun Manajemen Keselamatan Kebakaran Gedung (MKKG) termasuk SOP evakuasi;
b. menyediakan peralatan kebakaran yang mencakup alat pemadam api ringan, alat deteksi panas/asap, *water sprinkler*, dan alarm kebakaran di setiap lantai atau ruangan.
c. meletakkan Alat Pemadam Api Ringan pada tempat yang mudah dilihat dan dijangkau;
d. memeriksa dan merawat peralatan kebakaran secara rutin;
e. memastikan pintu dan tangga darurat tidak terhalang oleh benda apapun.
f. melakukan pemeriksaan ruangan penyimpanan bahan-bahan yang mudah terbakar secara berkala seperti ruang arsip;
g. memasang tanda-tanda petunjuk *Emergency Exit* dan *Escape Route* yang jelas pada setiap lantai;
h. menghindari tindakan-tindakan yang dapat menyebabkan terjadinya kebakaran, antara lain tidak membuang puntung rokok sembarangan, kelalaian penggunaan alat-alat listrik, serta hal-hal lain yang menyebabkan kebakaran;
i. menjauhkan benda-benda yang mudah terbakar seperti kertas, kain, atau bahan bakar dari api atau sumber api seperti kompor, arus listrik, rokok, dan sebagainya;
j. mematikan peralatan listrik dan kompor sebelum meninggalkan ruangan atau kantor;
k. melakukan pemeriksaan terhadap pusat-pusat sumber listrik, sumber daya listrik cadangan, saluran kabel listrik, gas dan sistem AC dan heater, genset dan tangki pasokan bahan bakar,

sistem proteksi petir, cerobong pembuangan asap secara periodik.

l. melaporkan untuk diadakan perbaikan jika menemukan kerusakan pada sumber listrik, sumber daya listrik cadangan, saluran kabel listrik, gas dan sistem AC dan heater, genset dan tangki pasokan bahan bakar, sistem proteksi petir, cerobong pembuangan asap;

m. menentukan *assembly point* yang posisinya berada pada jarak aman (kurang lebih 25 (dua puluh lima) meter dari gedung) jika diharuskan melakukan evakuasi akibat kebakaran;

n. melakukan latihan penanganan kebakaran dan evakuasi secara berkala, minimal 1 (satu) kali dalam setahun yang diikuti oleh seluruh personel;

o. melakukan koordinasi dengan Dinas Pemadam Kebakaran setempat untuk melakukan pemeriksaan sarana proteksi kebakaran gedung.

3. Penanggulangan Kebakaran

a. saat terjadi kebakaran, Kepala MKKG melakukan langkah-langkah sebagai berikut:
   1) Mengoordinasikan tim-tim MKKG melalui Posko yang telah ditentukan sebelumnya; dan
   2) Mencari informasi mengenai:
      a) lokasi api atau asap dan kondisinya;
      b) jumlah orang yang terperangkap;
      c) status evakuasi (sedang berjalan atau selesai);
      d) status api (dapat dipadamkan atau tidak); dan
      e) masalah yang dihadapi (contoh: tangga darurat terhalang benda).

b. Ketika mendengar alarm tanda kebakaran atau melihat sumber api dan/atau asap, Kepala MKKG menugaskan *floor warden* (komandan lantai) untuk melakukan hal-hal sebagai berikut:
   1) Memeriksa sub-panel alarm kebakaran untuk memeriksa sumber kebakaran;
   2) Menyiapkan proses evakuasi apabila kebakaran tidak berada pada lantai yang menjadi tanggung jawabnya;
   3) Apabila kebakaran berada di lantainya, segera laporkan kepada Posko jenis barang yang terbakar, lokasi tepatnya terjadi kebakaran, dan situasi terakhir.
   4) Melakukan koordinasi secara terus menerus dengan Tim MKKG.
   5) Memberi petunjuk, mengarahkan, dan mencarikan jalan keluar untuk para penghuni lantai tempat ia bertugas;
   6) Mengingatkan penghuni agar tidak menggunakan lift, mengarahkan penghuni ke pintu/tangga darurat terdekat; mengingatkan agar penghuni wanita yang memakai sepatu hak tinggi harap dilepas;

7) Menyelamatkan barang berharga atau dokumen penting ke tempat yang lebih aman yang telah ditentukan;
8) Menyerahkan barang atau dokumen tersebut kepada bagian pengamanan;
9) Memonitor situasi terakhir kebakaran;
10) Mengutamakan keselamatan jiwa daripada harta benda; dan

c. Tim Pemadam Kebakaran
1) Melakukan koordinasi dengan *floor warden* untuk mengetahui lokasi pasti terjadinya kebakaran;
2) Menuju ke tempat kejadian untuk memantau situasi (atas perintah Ketua Tim);
3) Memadamkan api dengan menggunakan APAR;
4) Memadamkan/melokalisasi kebakaran sebelum Petugas Pemadam datang;
5) Memberikan informasi kepada Ketua Tim secara terus menerus;
6) Melakukan koordinasi dengan Tim MKKG lainnya.
7) Memadamkan api dengan hidran Gedung apabila api tidak dapat dipadamkan dengan APAR; dan
8) Mempertahankan upaya pemadaman sambil menunggu bantuan dari Tim yang lain.

d. Tim Evakuasi
1) Membantu pemadaman di TKP;
2) Melakukan koordinasi secara simultan dengan Tim MKKG yang lain;
3) Mengadakan pencarian terhadap korban dan sumber api;
4) Membuka akses untuk pemadaman; dan
5) Menyisir semua lantai dari lantai teratas sampai lantai terbawah dan melaporkan situasi semua lantai yang disisir kepada Ketua Tim MKKG.

e. Tim P3K/Kesehatan
1) Melakukan koordinasi untuk meminta pelayanan bantuan medis;
2) Melakukan pertolongan dengan cepat dan tepat apabila ada korban; dan
3) Membawa korban ke rumah sakit apabila memerlukan perawatan medis lebih lanjut.

f. Tim Teknis
1) Mengatur dan mengontrol peralatan mekanik atau elektrik (lift, alarm, hidran, lampu darurat, peralatan evakuasi, dll);
2) Memutus zona lantai yang terbakar; dan
3) Membantu kelancaran tugas Pemadam Kebakaran yang datang.

g. Tim komunikasi
   1) Menghubungi Pemadam Kebakaran dan instansi terkait (atas perintah Ketua Tim) secepatnya; dan
   2) Membaca/mengumumkan teks 1, 2, 3, 4 atas perintah Kepala MKKG (1: siaga; 2: evakuasi tahap pertama; 3: evakuasi tahap kedua; 4: evakuasi total).

Prosedur Penanggulangan Kebakaran Dalam Jam Kerja.

a. Penanggulangan kebakaran kecil/awal.

   1) Melaporkan sumber api atau asap kepada *floor warden.*
   2) Memadamkan api dengan APAR yang tersedia di lantai tersebut.
   3) Apabila api belum dapat dipadamkan, maka melakukan langkah-langkah sebagai berikut:
      a) *Floor warden* melakukan koordinasi dengan Posko;
      b) *Floor warden* mengarahkan dan memimpin Regu Pemadam Kebakaran di lantainya untuk berusaha memadamkan api dengan menggunakan hidran yang terpasang di lantai tersebut;
      c) Regu Evakuasi dan Regu Penyelamat Lantai menyiapkan kemungkinan evakuasi dan penyelamatan jiwa dan/atau dokumen; dan
      d) Setelah api berhasil ditangani, *floor warden* melapor kepada Posko.

b. Penanggulangan Kebakaran Besar.

   1) *Floor Warden* (Komandan Lantai)
      Bila kebakaran tidak dapat dikuasai oleh Regu Pemadam Lantai, yang selanjutnya dilakukan adalah:
      a) Menyalakan alarm kebakaran;
      b) Melaporkan terjadinya kebakaran kepada kepala MKKG; dan
      c) Melakukan koordinasi dengan Tim MKKG dalam pelaksanaan evakuasi personel di lantainya serta menyelamatkan dokumen penting.

   2) Komandan Gedung
      Setelah Komandan Gedung menerima informasi kebakaran baik melalui laporan Komandan Lantai maupun dari alarm, maka Komandan Gedung:
      a) Memerintahkan semua penghuni gedung tetap tenang dan mengumumkan lokasi terjadinya kebakaran;
      b) Melakukan koordinasi evakuasi personel melalui komandan-komandan lantai, mulai dari atas lantai

yang terbakar sampai dengan lantai yang teratas, disusul dengan evakuasi personel mulai dari bawah lantai yang terbakar sampai dengan lantai yang terbawah;

c) Bekerja sama dengan Kepala Pasukan Pemadam Inti guna pengarahan personel serta peralatan kebakaran dan pengamanan yang diperlukan dalam usaha penanggulangan kebakaran (memadamkan, melokalisasi untuk mencegah meluasnya kebakaran serta bahaya-bahaya lain yang mungkin timbul, evakuasi personel dan penyelamatan jiwa atau harta benda);

d) Mengoordinasikan regu pemadam kebakaran lantai lainnya yang dapat diperbantukan dalam usaha penanggulangan kebakaran tersebut; dan

e) Melaporkan informasi tentang terjadinya kebakaran tersebut serta tindakan yang telah diambil dalam rangka penanggulangannya kepada kepala MKKG.

3) Teknisi

Setelah teknisi menerima informasi kebakaran baik melalui laporan komandan gedung maupun melalui alarm, maka selanjutnya teknisi melakukan:

a) Memberi instruksi atau saran-saran kepada Komandan Gedung dan Kepala Pasukan Pemadam Inti mengenai kemungkinan pengarahan personel dan peralatan yang diperlukan dalam rangka penanggulangan tersebut;

b) Memberi instruksi atau saran kepada fungsi penunjang (keamanan, teknisi, medis, dan logistik) dalam rangka membantu kelancaran penaggulangan kebakaran;

c) Menghubungi Dinas Kebakaran dan SAR guna mendapatkan bantuan bila diperlukan; dan

d) Melaporkan terjadinya kebakaran tersebut kepada kepala MKKG.

Prosedur Penanggulangan Kebakaran di Luar Jam Kerja.

1. Posko pengamanan
   a. Komandan atau Pengawas Posko bertindak sebagai Kepala Pemadam Kebakaran;
   b. Melakukan pemadaman api dengan fasilitas yang ada (APAR, hidran, atau tabung air);
   c. Apabila kebakaran tersebut telah dapat diatasi segera dibuatkan Berita Acara;
   d. Mengevakuasi diri serta semua orang yang masih berada di lingkungan gedung ke *assembly point*; dan

e. Apabila terjadi kebakaran besar segera menghubungi Dinas Kebakaran setempat untuk meminta bantuan.

2. Petugas jaga lain

Petugas jaga lain seperti petugas keamanan, teknisi, atau Personel yang masih berada di lingkungan Gedung agar membantu kelancaran penanggulangan kebakaran.

5. Petunjuk Pemilihan Alat Pemadam Api Ringan (APAR)

Pilih yang sesuai	Zat Kimia Kering (*Dry Chemical*)			CO_2	Halon	Air	Zat Kimia Basah (*Wet Chemical*)	
	Multi Purpose	Sodium bicarbonat	Purple K	Carbon dioxide	Halon 1211	Water	Pump tank	Loaded Stream (Stored pressured)
	Serba guna	$NaHCO_3$		CO_2		Air bertekanan	Tanki & pompa	Busa bertekanan
A	Ya	Tidak	Tidak	Tidak	Tidak	Ya	Ya	Ya
B	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Ya
C	Ya	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
	Bekerja dengan cepat Disarankan tersedia pada Gudang bahan bakar minyak dan gas, mobil serta bahan mudah terbakar lainnya			Bahan ini tidak meninggalkan bekas. Sesuai untuk alat elektronik dan Gudang bahan makanan		Murah, sesuai untuk bahan bangunan, rumah, Gedung, sekolah, perkantoran, dsb.		Sesuai untuk lab dan tempat bahan kima
	Lepas pena kunci, genggam handel & arahkan moncong di bawah api			Lepas pena kunci, genggam handel & arahkan moncong ke sumber api		Lepas pena kunci, genggam handel, guyur bahan terbakar	Pegang moncong, pompa, guyur bahan terbakar	Lepas pena kunci, genggam handel, guyur bahan terbakar

C. STANDAR OPERASIONAL PROSEDUR PENGAMANAN PERSONEL

Langkah-langkah yang perlu dilakukan personel dalam mengantisipasi ancaman-ancaman berikut:

1. Perampokan

a. Melakukan pemetaan dan menghindari tempat-tempat yang dinilai rawan di sekitar Kementerian dan/atau Perwakilan;

b. Tidak membawa uang, kunci dan dokumen pribadi dalam tempat yang sama;
c. Memastikan barang berharga berada dalam pengawasan;
d. Tidak membawa uang tunai dan/atau memakai perhiasan secara berlebihan;
e. Membawa tas dalam keadaan tertutup dengan tali tas melintang badan dan dipegang di bagian depan agar mudah diawasi;
f. Tidak melakukan penarikan uang di Bank sendirian, mengganti hari dan jam penarikan, maupun rute kedatangan/kepergian ke Bank, dan segera kembali ke Kementerian atau Perwakilan setelah melakukan pengambilan;
g. Melakukan pemetaan berbagai rute yang dapat dilalui sebelum bepergian;
h. Memperhatikan lingkungan sekitar untuk melihat apakah ada hal-hal yang mencurigakan, jika berada di bank untuk mengambil uang, sebelum keluar bank. Jika melihat ada hal-hal yang mencurigakan, jangan ragu-ragu untuk melaporkan ke pihak pengamanan Bank;
i. Langsung menaiki kendaraan dinas yang telah disiapkan untuk kembali ke kantor. Pastikan pintu dan jendela dalam keadaan terkunci, serta tas berisi uang tunai dalam posisi aman;
j. Melengkapi diri dengan sarana komunikasi yang memadai;
k. Memperhatikan kaca spion untuk melihat apakah kendaraan dinas/staf diikuti orang. Jika terdapat kecurigaan ada kendaraan yang mengikuti, kurangi kecepatan sedikit untuk melihat apakah mobil di belakang ikut mengurangi kecepatan. Kemudian tambah kecepatan untuk melihat apakah mobil di belakang ikut menambah kecepatan. Jika mobil di belakang masih mengikuti, ubah rute dengan berbelok, dan perhatikan apakah masih tetap diikuti. Apabila mobil penguntit tetap ada, hubungi aparat keamanan atau bawa kendaraan ke kantor polisi terdekat;
l. Melakukan pengamanan mandiri seperti bepergian dalam rombongan secara beriringan. Apabila diperlukan, bepergian dengan pengawalan atau pegawai setempat yang memahami bahasa setempat dan/atau melengkapi diri dengan senjata; dan
m. Menyiapkan nomor kontak darurat yang setiap saat dapat dihubungi jika terjadi keadaan yang tidak diinginkan.

2. Penculikan

a. Melakukan pemetaan dan menghindari tempat-tempat yang dinilai rawan di sekitar Kementerian dan/atau Perwakilan;
b. Apabila analisis risiko menunjukkan tingkat atau rasio penculikan yang tinggi, hindari bepergian sendiri ke wilayah yang rawan atau berbahaya. Apabila harus melakukan perjalanan melewati daerah rawan, lakukan pengamanan mandiri seperti bepergian dalam rombongan secara beriringan. Apabila daerah

tersebut berbahaya, menggunakan pengawalan personel keamanan yang disewa dan/atau personel pengamanan yang disediakan pemerintah setempat;

c. Menghindari bepergian sampai larut malam, membawa uang tunai dan memakai perhiasan yang berlebihan, jalan yang sarana penerangannya kurang pada malam hari atau jalan/tempat parkir yang sepi;
d. Mengenali lingkungan sekitar dan *escape route* setiap memasuki lingkungan yang baru. Menyiapkan rencana melarikan diri sebelum memasuki wilayah yang rawan/berbahaya;
e. Menggunakan rute/jalan yang ramai. Menghindari penggunaan rute perjalanan yang sama pada saat pergi atau pulang dari/ke tempat tujuan. Mempelajari berbagai rute yang dapat ditempuh ke tujuan;
f. Melengkapi diri dengan sarana komunikasi yang memadai dan menyiapkan nomor kontak darurat/aparat keamanan di wilayah yang dikunjungi;
g. Menginformasikan rencana perjalanan ke luar kantor (terutama ketika jarak yang ditempuh jauh dan dalam rangka dinas) kepada personel lain. Memperhatikan *travel advisory* jika ada;
h. Jika dirasa perlu, melengkapi diri dengan peralatan yang dapat dipakai untuk mempertahankan diri;
i. Menyiapkan kendaraan yang akan dipakai selama bepergian dalam keadaan yang laik jalan;
j. Melengkapi perjalanan dengan asuransi perjalanan (apabila tersedia) dengan mempertimbangkan risiko-risiko seperti situasi keamanan, kondisi perjalanan menuju lokasi dan sebagainya; dan
k. Menghindari perselisihan dengan warga setempat.

3. Tindakan Kekerasan Fisik

a. Menghindari bepergian sampai larut malam, menghindari jalan/daerah yang sarana penerangannya kurang pada malam hari;
b. Menghindari bepergian ke daerah rawan/berbahaya;
c. Lakukan pengamanan mandiri seperti bepergian dalam rombongan. Jika hal ini tidak memungkinkan, pesan taksi/sarana transportasi lainnya yang aman;
d. Apabila yakin diikuti seseorang, mengamati wajah/mata orang tersebut. Hal ini berguna untuk menandakan bahwa kita mengetahui apa yang sedang terjadi. Memperhatikan semua ciri-ciri orang tak dikenal tersebut; dan
e. Apabila diikuti orang tak dikenal, segera mencari tempat aman seperti tempat yang ramai orang. Menginformasikan lokasi kepada personel lain atau menghubungi aparat keamanan terdekat.

4. Penggalangan dan Agitasi

   a. Mengadakan seleksi ketat baik pada saat penerimaan pegawai honorer atau pegawai *outsourcing* di Kementerian, maupun *local staff* atau pegawai honorer di Perwakilan. Perumusan kontrak kerja sebaiknya memuat klausul pencegahan terhadap penggalangan dan agitasi;
   b. Memastikan bahwa personel yang telah berakhir kontrak kerjanya tidak lagi memiliki akses masuk ke gedung atau data Kementerian dan/atau Perwakilan;
   c. Menerapkan zonasi akses terutama akses bagi pekerja kontrak/honorer dan tamu asing ke tempat-tempat strategis;
   d. Menggunakan pintu elektronik yang dapat diakses hanya dengan kartu akses atau biometrik;
   e. Mendampingi dan mengawasi pekerja kontrak/pekerja perusahaan penyedia jasa (penyedia air mineral, petugas kebersihan, dan sebagainya);
   f. Memberikan pembekalan secara berkala kepada seluruh personel beserta seluruh anggota keluarganya mengenai potensi penggalangan dari pihak luar;
   g. Melakukan pengawasan kegiatan yang dilakukan oleh seluruh personel dan tamu, terutama kegiatan mencurigakan seperti memasuki tempat yang tidak berhubungan dengan tugas dan fungsi pada jam-jam tertentu, melanggar prosedur keamanan secara berulang-ulang, atau mencari informasi tertentu yang tidak berhubungan dengan tugas dan fungsi;
   h. Menegakkan peraturan/ketentuan hukum yang berlaku secara konsisten;
   i. Melakukan komunikasi yang bersifat kedinasan secara hati-hati untuk menghindari upaya penggalangan, agitasi serta kebocoran informasi; dan
   j. Menggunakan media sosial secara beretika dan bertanggung jawab.

5. Kecelakaan Kerja

   a. Menyusun prosedur kesehatan dan keselamatan kerja dalam menghadapi keadaan darurat, bencana dan insiden lainnya;
   b. Memperhatikan dan menganalisis risiko pekerjaan yang dilakukan Kementerian dan Perwakilan;
   c. Memastikan fasilitas gedung sesuai dengan standar;
   d. Memasang rambu-rambu keselamatan dan pintu darurat;
   e. Menyediakan fasilitas P3K;
   f. Memasang nomor kontak darurat untuk pertolongan medis ditempat yang mudah terlihat; dan
   g. Mempersiapkan peralatan pendukung yang dibutuhkan untuk membantu pelaksanaan kerja yang bersifat fisik (masker, *trolley*, sarung tangan, tuas pengangkat, dan sebagainya).

6. Penyakit Endemik

   a. Mengikuti perkembangan penyebaran penyakit di wilayah Republik Indonesia dan di negara akreditasi melalui media;
   b. Melakukan koordinasi dengan otoritas terkait mengenai penyebaran penyakit endemik;
   c. Menghindari bepergian ke lokasi yang berpotensi penyakit endemik, kecuali terkait perlindungan Warga Negara Indonesia;
   d. Memastikan seluruh personel telah divaksinasi sesuai dengan kebutuhan; dan
   e. Menyiapkan rencana penanganan dalam rangka pencegahan penyebaran penyakit endemik.

7. Perubahan Kondisi Alam

   a. Memperhatikan perkembangan perubahan kondisi alam di Indonesia maupun di negara akreditasi melalui media dan otoritas terkait;
   b. Menghindari akses ke lokasi yang berpotensi mengancam keselamatan jiwa personel, kecuali terkait dengan perlindungan Warga Negara Indonesia; dan
   c. Memiliki *contingency plan* bencana alam terutama jika menurut analisis risiko, wilayah kerja memiliki potensi bencana alam tinggi.

D. STANDAR OPERASIONAL PROSEDUR PENGAMANAN INFORMASI

Pengamanan Informasi adalah suatu upaya yang terencana, terarah, terpadu, dan berkesinambungan untuk melindungi dan meminimalisir resiko akibat ancaman terhadap aset informasi Perwakilan RI yang mungkin terjadi. Sistem Pengamanan informasi dimaksudkan untuk mencapai tiga tujuan utama yaitu; *kerahasiaan, ketersediaan dan integritas.*

- Kerahasiaan. Sistem pengamanan harus melindungi data dan informasi sesuai klasifikasinya dari pengungkapan kepada pihak-pihak yang tidak berwenang dan dari ancaman-ancaman yang disebabkan oleh *human error,* pencurian, serangan *hacker* dan lain sebagainya.

- Ketersediaan. Sistem pengamanan harus dapat menjamin pengguna dapat mengakses data dan informasi kapanpun dibutuhkan.

- Integritas. Sistem pengamanan harus dapat menjamin kelengkapan informasi dan menjaga dari korupsi, kerusakan, atau ancaman lain yang menyebabkan berubah informasi dari aslinya.

1. PENGAMANAN PENGGUNAAN PERANGKAT BERGERAK DAN *TELEWORKING*

   a) tidak meninggalkan peralatan yang memuat informasi sensitif maupun kritikal baik sengaja maupun tidak sengaja;
   b) menggunakan kata kunci/sandi, pin, atau pola pada peralatan yang memuat informasi sensitif maupun kritikal;
   c) tidak memasang aplikasi yang ilegal atau dari sumber yang tidak valid pada perangkat bergerak;
   d) melakukan *update* terhadap sistem operasi perangkat bergerak.
   e) menggunakan antivirus dan *firewall* pada perangkat bergerak yang digunakan untuk *teleworking*;
   f) menerapkan kriptografi, mencatat dan memonitor akses *teleworking*; dan
   g) mencabut hak akses apabila aktivitas *teleworking* sudah selesai.

2. PENGAMANAN PERSONEL TERKAIT KEAMANAN INFORMASI

   a) menerapkan keamanan informasi sesuai dengan kebijakan dan prosedur yang ada di Kementerian dan Perwakilan;
   b) memberikan pengertian dan penyadaran tentang peran dan tanggung jawab terkait akses terhadap informasi maupun sistem informasi;
   c) memberikan pendidikan, pelatihan dan sosialisasi tentang keamanan informasi secara berkala sesuai tingkat tanggung jawabnya;
   d) memberikan sosialisasi kepada pihak eksternal untuk meningkatkan keamanan informasi dan pembaruan terhadap kebijakan keamanan informasi Kementerian dan Perwakilan; dan
   e) pihak eksternal harus menandatangani *non-disclosure agreement* sebelum melakukan akses terhadap informasi.

3. PENGELOLAAN ASET TERKAIT KEAMANAN INFORMASI

   a) memastikan bahwa setiap aset yang dikelola jelas kepemilikannya;
   b) mengklasifikasikan informasi yang dikelola sesuai dengan nilai sensitivitas dan tingkat risiko atau sesuai dengan peraturan perundangan yang berlaku;
   c) memberikan label terhadap setiap informasi baik secara fisik maupun elektronik untuk memastikan penanganan informasi sesuai prosedur yang berlaku;
   d) mengindentifikasi dan menginventarisasi seluruh informasi atau aset yang berkaitan dengan informasi;
   e) menyimpan seluruh media yang menyimpan informasi pada tempat yang aman;

f) memusnahkan dan menghancurkan seluruh informasi pada media yang melewati masa retensi; dan
g) memastikan seluruh informasi yang ada di dalam aset yang sudah tidak dimiliki atau digunakan oleh Kementerian atau Perwakilan, telah terhapus ketika selesai masa kontrak.

4. PENGENDALIAN AKSES

a) menentukan aturan kontrol akses yang tepat, sesuai dengan hak akses dan pembatasan untuk peran pengguna tertentu;
b) memberikan hak akses terhadap jaringan kepada personel sesuai dengan tugas dan tanggungjawabnya;
c) mencatat semua proses pendaftaran, perubahan serta pencabutan hak akses;
d) mengindentifikasi alokasi hak akses pada setiap sistem atau proses contohnya sistem operasi, basis data, setiap aplikasi dan pengguna;
e) melakukan penonaktifan dan pencabutan hak akses terhadap informasi maupun peralatan pengolah informasi kepada personel maupun pihak eksternal yang sudah pensiun/tidak bekerja/selesai kontrak;
f) mengubah informasi autentikasi rahasia yang dibuat oleh pihak eksternal setelah pemasangan sistem atau perangkat lunak selesai;
g) melakukan reviu terhadap kontrol akses terhadap suatu aset secara periodik;
h) menjaga kerahasiaan kata kunci/sandi. Memastikan informasi tersebut tidak diungkap kepada pihak lain oleh pengguna; dan
i) melakukan prosedur *log in* yang aman terhadap sistem, aplikasi maupun kode sumber.

5. PENGAMANAN LINGKUNGAN DAN FISIK

a) menentukan pembagian parameter area pengamanan untuk melindungi area yang menyimpan informasi sensitif maupun kritikal;
b) tidak membawa peralatan fotografi, video, audio atau alat perekam lainnya, kecuali diizinkan dan tercatat;
c) membatasi dan memonitor akses ke area dimana informasi rahasia/terbatas diproses atau disimpan;
d) menyimpan informasi terbatas/rahasia dalam bentuk kertas maupun media penyimpanan pada tempat yang terkunci pada saat tidak digunakan;
e) meninggalkan komputer dalam keadaan *logged off* /terkunci pada saat tidak digunakan; dan

f) memastikan seluruh personel dan tamu memakai tanda pengenal ketika memasuki area pengolahan/penyimpanan informasi.

6. PENGAMANAN KEGIATAN OPERASIONAL

a) melakukan instalasi, sistem konfigurasi, pencadangan, dan *monitoring* sesuai prosedur;
b) mendokumentasikan setiap perubahan pada proses bisnis, infrastruktur, maupun seluruh sistem yang mempengaruhi informasi;
c) menyiapkan prosedur pemulihan sebelum melakukan perubahan untuk mencegah gagalnya sistem;
d) memonitor penggunaan sumber daya, dan membuat perkiraan kebutuhan kapasitas kedepan untuk memastikan kinerja perangkat;
e) membuat dan menyimpan secara reguler catatan kejadian yang berisi rekaman aktivitas pengguna, kegagalan dan kejadian keamanan informasi untuk kebutuhan evaluasi;
f) melakukan *updating* perangkat lunak operasional, aplikasi dan program secara berkala;
g) memisahkan antara lingkungan pengembangan, pengujian dan operasional sistem operasi untuk meminimalisasi akses yang tidak berhak dan/atau gangguan pada sistem yang sedang berjalan;
h) memastikan ketersediaan informasi tentang kerentanan teknis sistem informasi yang digunakan ketika dibutuhkan;
i) mengevaluasi kerentanan informasi untuk mengukur dan mengatasi risiko dengan tepat;
j) melaksanakan penanganan dan pemulihan sistem dari gangguan sesuai prosedur; dan
k) menggunakan satu sumber yang sama dalam pengaturan waktu pada seluruh peralatan fasilitas pemrosesan informasi.

7. PENGAMANAN KOMUNIKASI

a) mengatur dan mengontrol jaringan untuk melindungi informasi pada sistem dan aplikasi;
b) merekam dan mendeteksi kegiatan yang dapat berpengaruh, atau yang berhubungan dengan keamanan informasi;
c) membatasi sistem yang terhubung dengan jaringan sesuai dengan fungsinya;
d) mengindentifikasi mekanisme keamanan tingkat layanan dan kebutuhan pada seluruh layanan jaringan;
e) menerapkan teknologi jaringan untuk dapat melakukan kontrol terhadap jaringan sesuai standar pengamanan;

f) melakukan pengelompokan layanan informasi, pengguna dan sistem informasi;
g) menerapkan teknik kriptografi sesuai dengan tingkat kerentanan risiko keamanan pada informasi yang ditransfer dalam proses komunikasi; dan
h) tidak melakukan pembicaraan yang berklasifikasi terbatas/rahasia pada tempat yang terbuka.

8. PENGAMANAN INFORMASI DALAM PENGADAAN, PENGEMBANGAN DAN PEMELIHARAAN SISTEM INFORMASI

a) mengontrol perubahan dalam proses pengembangan sesuai ketentuan yang berlaku;
b) menyesuaikan perubahan dokumentasi operasional dan prosedur pengguna dengan kebutuhan;
c) memonitor pengembangan yang dilakukan oleh pihak eksternal;
d) mencantumkan kebutuhan desain keamanan, kode sumber dan uji coba pada dokumen kontrak dengan pihak eksternal;
e) membuat dokumen bukti uji coba untuk mencegah kerawanan;
f) menerapkan uji coba fungsi keamanan pada saat pembangunan;
g) melaksanakan program uji keberterimaan dan kriteria yang berhubungan pada saat implementasi sistem informasi yang baru atau *upgrade* sistem atau versi baru; dan
h) memilih data yang digunakan untuk uji coba secara hati-hati.

9. PENGAMANAN INFORMASI TERHADAP HUBUNGAN DENGAN PIHAK EKSTERNAL

a) mematuhi SOP dan siklus hidup dalam pengaturan hubungan dengan pihak eksternal;
b) mengidentifikasi kriteria pihak eksternal yang dapat diberikan izin untuk mengakses informasi;
c) mengawasi pekerjaan pihak eksternal sesuai prosedur;
d) membuat daftar kebutuhan keamanan informasi yang harus dipatuhi oleh pihak eksternal dalam mengakses, memproses, menyimpan, mengkomunikasikan, atau memberikan komponan Infrastruktur teknologi informasi dan komunikasi di lingkungan Kementerian dan Perwakilan;
e) memastikan pihak eksternal mematuhi seluruh prosedur keamanan di lingkungan Kementerian dan Perwakilan; dan
f) memantau dan mengevaluasi seluruh kegiatan pihak eksternal secara reguler.

10. PENGELOLAAN INSIDEN KEAMANAN INFORMASI

a) menetapkan dokumen prosedur persiapan, perencanaan dan penanganan dalam respon terhadap insiden keamanan informasi;

b) melaporkan setiap insiden keamanan informasi kepada Komite Pengamanan atau Tim Pengamanan;
c) menangani insiden keamanan informasi sesuai ketentuan; dan
d) mendokumentasikan penanganan insiden keamanan informasi.

11. KEAMANAN INFORMASI DALAM PENGELOLAAN KEGIATAN

a) memastikan dan menguji ketersediaan dari sistem informasi yang ada;
b) menyusun rencana kontijensi untuk menjaga layanan informasi;
c) melakukan simulasi keadaan darurat secara berkala untuk memastikan layanan sistem informasi masih dapat berjalan ketika terjadi insiden atau bencana; dan
d) memasang fasilitas pemrosesan informasi sesuai kebutuhan.

II. DAFTAR KELENGKAPAN DAN SPESIFIKASI SARANA DAN PRASARANA PENGAMANAN

A. Umum

Prinsip penyediaan sarana dan prasarana pengamanan pada Kementerian dan Perwakilan dilakukan dengan mempertimbangkan keseimbangan antara aspek keamanan, kenyamanan, kebutuhan, ketersediaan anggaran dan peraturan perundang-undangan.

B. Sistem Manajemen Pengamanan

Standar Operasional Prosedur (SOP)	
Keterangan	Kementerian dan Perwakilan harus memiliki SOP mengenai: Manajemen Keselamatan Kebakaran Gedung (MKKG), Rencana Kontijensi, Pencegahan Gangguan Keamanan, Penanganan Unjuk Rasa, Tim Pengamanan dan Pengamanan Pengelolaan Keuangan
Standar Minimal	SOP tersebut harus dikukuhkan dengan Surat Keputusan (SK)
Kuantitas	Masing-masing 1 (satu) SOP
Ketentuan Khusus	1. Kementerian dan Perwakilan harus menyelenggarakan sosialisasi mengenai SOP dimaksud, secara berkala; 2. Kementerian dan Perwakilan harus menyusun Struktur Organisasi dan uraian tugas dari Tim MKKG dan *floor captains,* Kontijensi, Pencegahan

	Gangguan Keamanan, Penanganan Unjuk Rasa, Tim Pengamanan dan Pengamanan Pengelolaan Keuangan; 3. Kementerian dan Perwakilan harus menyusun mekanisme koordinasi internal dan eksternal. Mekanisme tersebut harus melibatkan semua unsur Kementerian dan/atau Perwakilan serta aparat keamanan setempat; 4. Kementerian dan Perwakilan harus menyelenggarakan kegiatan latihan secara berkala untuk memastikan semua Personel mengetahui tugas masing-masing saat SOP diberlakukan.

C. Standar Pengamanan Aset Fisik

1) Kantor Kementerian dan Perwakilan

Keberadaan infrastruktur fisik yang dibutuhkan oleh Kementerian dan Perwakilan, baik eksterior maupun interior, didasarkan pada kebutuhan untuk menciptakan lingkungan yang dapat mencegah dan merespon potensi ancaman dan gangguan. Standar infrastruktur pengamanan fisik dimaksud yaitu:

Zonasi Akses	
Ruang Terbatas	Ruang Tertutup
1. Ruang kerja Pimpinan 2. Ruang kerja Personel 3. Ruang Pelayanan Publik 4. Ruang Pertemuan 5. Posko Pengamanan 6. Ruang Tamu 7. Lobi Penerimaan Tamu	1. Ruang Penyimpanan peralatan Teknologi Informasi dan Komunikasi. 2. Ruang Arsip 3. Ruang Penyimpanan Uang dan Dokumen berklasifikasi Rahasia 4. Ruang Monitor dan penyimpanan Data Rekaman CCTV

Gerbang	
Keterangan	Gerbang masuk dan keluar gedung sebaiknya terpisah. Hal ini bertujuan sebagai jalur alternatif saat keadaan darurat atau jalur evakuasi tambahan/cadangan.
Standar Minimal	Terpisah antara gerbang masuk dan keluar
Kuantitas	2 (dua)

Ketentuan Khusus	• Dapat dilewati oleh mobil pemadam kebakaran. • Gerbang dilengkapi dengan *gate barrier*.

Pagar	
Keterangan	Berfungsi sebagai *deterrent* untuk mencegah atau menghambat pihak penyusup ke lingkungan Kementerian dan Perwakilan.
Standar Minimal	Memiliki ketinggian minimal 3 meter dan bahan yang kokoh.
Kuantitas	Mengelilingi perimeter Kementerian dan/atau Perwakilan.
Aspek pengamanan tambahan	Dapat dilengkapi dengan kawat berduri atau *fiber glass*, dan dapat diganti dengan dinding (*concrete wall*).



Keberadaan pagar dan gerbang dapat dikecualikan pada beberapa Perwakilan dengan kondisi tertentu (sewa gedung atau hotel) seperti KJRI Hongkong dan KJRI Guangzhou, atau karena keterbatasan lain seperti KJRI New York.

Lampu Penerangan Halaman	
Keterangan	Mengurangi potensi gangguan serta membantu proses pengawasan lingkungan kantor Perwakilan.
Standar Minimal	• memiliki intensitas tinggi. • menerangi seluruh bagian halaman.
Kuantitas	Diletakkan pada tempat-tempat strategis.
Ketentuan Khusus	Lampu penerangan digunakan sebagai penerangan halaman kantor dan menerangi *perimeter* luar gerbang, sekeliling pagar, dan area yang disorot CCTV.

Pintu Masuk Kantor	
Keterangan	Akses keluar masuk orang ke dalam gedung.
Standar Minimal	Dapat berupa pintu manual (kunci, gembok) atau otomatis (RFID, *Fingerprint, biometric, access card*).
Kuantitas	Minimal 2 (dua) pintu utama untuk memisahkan akses antara personel dan umum
Ketentuan Khusus	• Engsel pada pintu manual diletakkan di sisi dalam. • Perlu pintu tambahan untuk *loading* barang yang terpisah dari akses masuk orang.

Pintu Darurat	
Keterangan	Pintu berfungsi sebagai jalur untuk keluar dari gedung pada situasi darurat (kebakaran, unjuk rasa, serangan teror, bencana)
Standar Minimal	• Dapat berupa pintu manual (kunci, gembok) atau otomatis (RFID, *Fingerprint, biometric, access card*) • Letak pintu agar terpisah dari pintu gerbang masuk
Kuantitas	Minimal 1 (satu)
Ketentuan Khusus	• Engsel pada pintu manual diletakkan di sisi dalam. • Memiliki mekanisme koordinasi untuk membuka pintu darurat apabila berbatasan langsung dengan areal milik orang lain.



Jenis-jenis mekanisme penguncian pintu

Teralis Pengaman	
Keterangan	Merupakan alat pengaman tambahan bagi pintu/jendela gedung, terutama untuk kantor yang tidak memiliki pagar.
Standar Minimal	Terbuat dari bahan besi atau baja dengan diameter minimal 10 mm atau plat dengan ketebalan minimal 3 mm dan lebar minimal 2 cm.
Kuantitas	Disesuaikan dengan jumlah pintu/jendela yang berhubungan langsung dengan area luar kantor, atau merupakan akses kedalam ruang strategis.
Ketentuan Khusus	Dalam keadaan darurat, dapat dibuka dari arah dalam.

Tangga Darurat	
Keterangan	Kantor Perwakilan yang memiliki lebih dari 2 (dua) lantai harus dilengkapi dengan tangga darurat.
Standar Minimal	• Terletak di bagian luar Gedung. • Tahan api. • Lebar minimal 90 cm. • Terhubung langsung ke area terbuka yang dapat diakses oleh pemadam kebakaran. • Dilengkapi dengan jendela atau lubang yang

	digunakan untuk proses evakuasi darurat, juga sebagai akses masuk alternatif bagi petugas pemadam kebakaran, serta *exhaust* untuk suplai udara. • Jarak terjauh ruang kerja menuju tangga darurat maksimum 25 meter.
Kuantitas	Minimal jumlah tangga darurat 2 (dua) untuk gedung bertingkat lebih dari 2 (dua) lantai atau luas lebih dari 500 m^2.
Ketentuan Khusus	• Tangga darurat harus memiliki penerangan yang cukup. • Tidak digunakan untuk menyimpan barang-barang yang menghalangi proses evakuasi. • Dapat dilengkapi dengan stiker *glow in the dark*. • Setiap pintu tangga darurat harus dilengkapi tanda/papan petunjuk bertuliskan *EXIT*/KELUAR.

Closed Circuit Television (CCTV)	
Keterangan	Alat bantu pengawasan lingkungan gedung secara *remote* atau jarak jauh.
Standar Minimal	CCTV tipe PTZ (*Pan Tilt Zoom*) dengan resolusi 720p dan 600 TVL.
Kuantitas	• Jumlah CCTV disesuaikan dengan kebutuhan dengan mempertimbangkan pengawasan seluruh titik rawan dan strategis. • Dapat menyorot perimeter di lingkungan kantor, dan area di sekeliling pagar dan luar pagar. • Dapat menyorot akses keluar/masuk di setiap lantai.
Ketentuan Khusus	CCTV harus dilengkapi dengan media penyimpanan yang dapat menampung data hasil rekaman selama 3 - 6 bulan.
Contoh	

Monitor CCTV	
Keterangan	Monitor CCTV merupakan bagian dari perangkat CCTV dengan *manufacturer* yang sama.
Standar Minimal	• Display minimal 600 TV. • Ukuran Monitor disesuaikan dengan jumlah CCTV, agar dapat menampilkan gambar yang jelas dalam waktu yang bersamaan.
Kuantitas	Monitor CCTV dapat dipantau dari ruang kontrol keamanan/Satpam, meja resepsionis, ruang pejabat komunikasi, serta ruang pejabat Perwakilan yang bertanggung jawab terhadap keamanan gedung.
Ketentuan Khusus	• Monitor CCTV tidak dapat dilihat oleh pihak luar (tamu). • Monitor CCTV agar menghindari sistem *remote* yang dapat diakses melalui IP Address dari luar KBRI, kecuali dapat dipastikan keamanannya dan akses penggunaannya.

Meja Resepsionis	
Keterangan	Sebagai tempat penerimaan dan pemberian informasi untuk tamu.
Standar Minimal	• Diletakkan di lokasi yang mampu mengawasi pergerakan keluar masuk tamu. • Terdapat monitor CCTV.
Kuantitas	Satu unit yang diletakkan sebagai *buffer* antara area akses terbatas dengan akses tertutup.
Ketentuan Khusus	• Meja resepsionis juga dilengkapi dengan buku tamu. • Penerimaan paket/dokumen sebaiknya tidak dilakukan di resepsionis, tetapi di *mailing room.* • Apabila terdapat monitor CCTV, maka harus dipastikan tidak dapat terlihat oleh orang luar atau tamu.

Pos Pengamanan	
Keterangan	Berfungsi sebagai pengendali pengamanan yang sifatnya taktis dan strategis.
Standar Minimal	Dilengkapi dengan *walkie-talkie*, senter, buku catatan kejadian, *portable metal detector*, *visitor card*, telepon, dan nomor kontak darurat.
Kuantitas	1 (satu) ruangan
Ketentuan Khusus	• Terletak pada lokasi strategis di dalam premis gedung atau tepat di samping gerbang masuk orang atau kendaraan. • Dapat memantau lingkungan gedung dan perimeter

	luar.

Lemari / Brankas Besi	
Keterangan	Digunakan untuk menyimpan dokumen, uang, alat sandi, dan senjata api.
Standar Minimal	• Menggunakan kunci manual atau kombinasi. • Tidak bisa diangkut oleh 2 (dua) orang. • Terbuat dari bahan tahan api (minimal selama 2 jam).
Kuantitas	Diletakkan di posisi yang aman dan tidak mudah terlihat.
Ketentuan Khusus	Dapat dipantau melalui CCTV.

Kotak Penyimpanan Kunci	
Keterangan	Tempat penyimpanan bagi seluruh kunci, termasuk pintu akses masuk dan keluar gedung, kunci tiap ruangan gedung, dan kunci kendaraan operasional.
Standar Minimal	Dapat menampung semua kunci dan tidak dapat dibongkar dengan mudah.
Kuantitas	1 unit diletakkan di ruangan penyimpanan khusus.
Ketentuan Khusus	Selama tidak digunakan agar dipastikan tetap dalam kondisi terkunci dan kuncinya dipegang oleh personel yang diberi tanggung jawab penyimpanan.

Sistem Proteksi Kebakaran	
Keterangan	Perangkat untuk mencegah dan meminimalisasi dampak kebakaran.
Standar Minimal	• Alat pemadam kebakaran ringan (APAR). • Hidran halaman dengan tenaga mesin dan memiliki sumber air baik dari reservoir atau dari sambungan perusahaan air setempat. • Hidran internal untuk gedung yang memiliki 4 lantai atau lebih. • *Sprinkler* . • Alarm kebakaran. • *Fire hose.* • *Smoke / fire detector.* • *Speaker*/pengeras suara yang menggunakan kabel tahan api. • Lampu darurat. • Petunjuk arah dan jalur evakuasi.

Kuantitas	• 2 (dua) tabung APAR untuk setiap lantai. • 1 (satu) hidran box untuk setiap lantai. • Minimal memiliki 1 (satu) hidran halaman.
Ketentuan Khusus	• Alarm kebakaran sebaiknya tersambung dengan dinas kebakaran setempat. • Perlu pemeriksaan berkala yang dilakukan oleh dinas kebakaran setempat. • APAR diletakkan di tempat-tempat strategis yang tidak terhalang oleh benda lain yang dapat menyulitkan pemadaman pada situasi darurat.
Contoh	 

Sumber Listrik Cadangan	
Keterangan	Sumber listrik cadangan wajib dimiliki agar sistem pengawasan dan pengamanan tetap dapat berjalan pada saat terjadi *blackout*.
Standar Minimal	Generator tipe *rectifier* dengan mesin 4 tak dan bahan bakar solar.
Kuantitas	Disesuaikan dengan jumlah daya yang dibutuhkan di kantor Perwakilan.
Ketentuan Khusus	• Generator harus ditempatkan di luar ruangan dan memiliki pagar pelindung, di mana ada udara yang cukup untuk mendinginkan generator dan ventilasi tidak terhalang apapun. • Generator harus ditempatkan pada permukaan, yang tidak mudah terbakar, seperti permukaan tanah dan letakan pondasi seperti kayu atau yang lainnya untuk mencegah kontak ketika air meluap. • Generator harus dipasang di dekat lokasi saklar transfer dan jauh dari tangki pasokan bahan bakar, untuk mengurangi pemasangan kabel dan pipa yang panjang, mungkin diperlukan adanya izin jika berniat untuk menyimpan tangki bahan bakar yang besar. • Genset harus ditempatkan terpisah dari gedung induk, dan diadakan pengujian rutin (tes beban) minimal 1 (satu) bulan sekali. • Genset harus bisa memenuhi kebutuhan listrik untuk hidrant dan lift dalam keadaan kebakaran untuk transportasi petugas kebakaran.

Sistem Instalasi Listrik	
Keterangan	Instalasi listrik yang baik dan terawat dapat mencegah terjadinya kebakaran akibat hubungan arus pendek.
Standar Minimal	- Beban daya listrik harus sesuai dengan kebutuhan. - Sistem instalasi listrik harus terencana dengan baik.
Kuantitas	Spesifikasi kabel dan sambungan listrik, panel (MCCB) sesuai dengan standar keamanan dan beban daya listrik.
Ketentuan Khusus	Pemeriksaan, pengujian dan pemeliharaan secara berkala.

Alat Pertolongan Pertama Pada Kecelakaan (P3K)	
Keterangan	Peralatan yang digunakan untuk memberikan pertolongan pertama pada personel/tamu yang mengalami gangguan kesehatan atau kecelakaan kerja.
Standar Minimal	• Kotak P3K diletakkan di tempat yang mudah dijangkau/area terbuka dan terlihat dengan jelas. • Kotak P3K harus mudah dikenali, misalnya dengan adanya logo palang merah/hijau, dan tulisan dengan ukuran besar.
Kuantitas	Satu set kotak P3K untuk jumlah personel <50 orang.
Ketentuan Khusus	Dapat dilengkapi dengan alat pacu jantung atau *defibrillator*, masker dan tabung oksigen.

Penunjuk Arah	
Keterangan	Alat bantu untuk menunjukkan arah ke jalur evakuasi dalam keadaan darurat.
Standar Minimal	Dibuat dari bahan yang tahan air dan tidak pudar, berukuran besar dan mudah dilihat.
Kuantitas	Sesuai kebutuhan.
Ketentuan Khusus	• Digunakan untuk memberitahukan arah atau letak dari tangga darurat, pintu darurat, alat pemadam kebakaran, titik kumpul (*assembly point*), zonasi akses dan alat kesehatan. • Dibuat dalam bahasa Indonesia dan bahasa lokal.

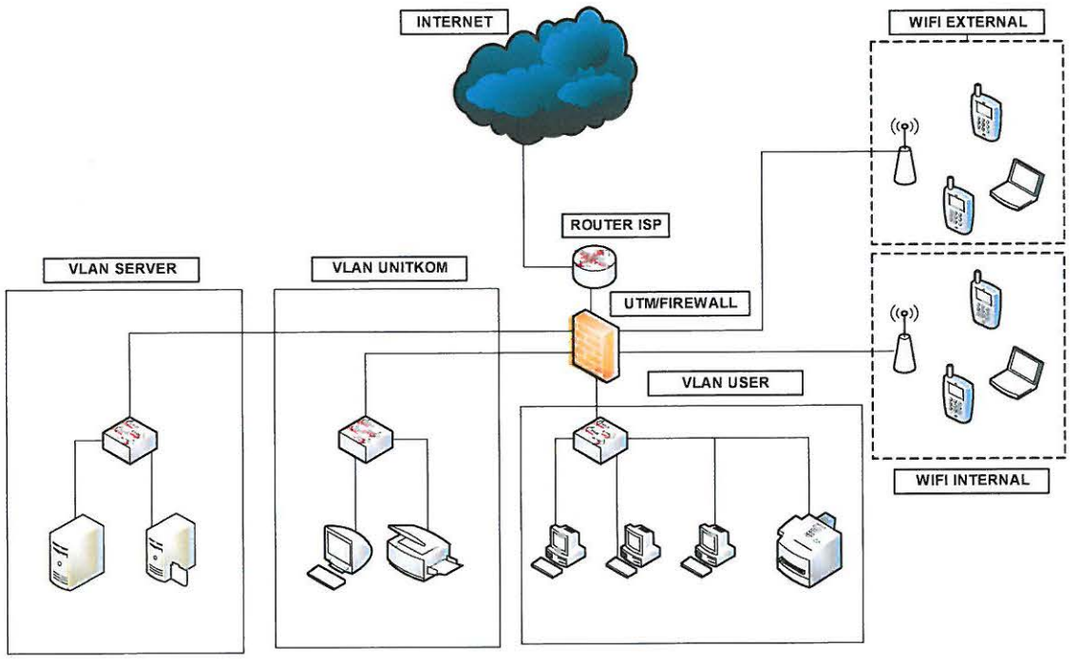
Sistem Alarm dan *Panic Button*	
Keterangan	Gedung dapat dilengkapi dengan beberapa jenis alarm, seperti alarm kebakaran, alarm pencurian dan *motion detector.*
Standar Minimal	• Alarm kebakaran terletak di setiap lantai. • *Motion detector* ditempatkan di dekat akses pintu dan jendela. • Instalasi *Panic Button* diletakkan di beberapa lokasi seperti Ruang Keppri, resepsionis, dan posko keamanan.
Kuantitas	Jumlah alarm disesuaikan dengan kondisi bangunan.
Ketentuan Khusus	• Alarm kebakaran terhubung dengan sistem proteksi kebakaran yang telah dipasang. • Alarm kebakaran terhubung dengan kantor pemadam kebakaran setempat. • Alarm pencurian terhubung dengan aparat kepolisian setempat atau penyedia jasa keamanan yang disewa. • Memeriksa keaktifan alarm secara berkala. • Perlu diperhatikan perawatan sistem alarm agar tidak menghasilkan *false alarm.*

2) Standar Minimal Pengamanan Wisma Kepala Perwakilan atau Wakil Kepala Perwakilan

Standar minimal yang telah disebutkan di atas juga berlaku untuk Wisma atau tempat tinggal Kepala Perwakilan atau Wakil Kepala Perwakilan dan bangunan lainnya yang menjadi aset Perwakilan, dengan catatan disesuaikan dengan kebutuhan dan aturan setempat.

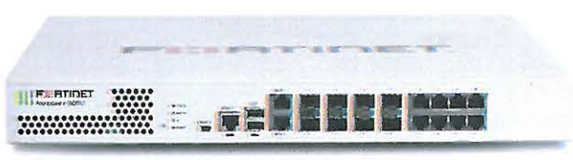
D. STANDAR PENGAMANAN INFORMASI

Topologi Jaringan	
Keterangan	Topologi didokumentasikan untuk digunakan dalam rangka pemeliharaan, evaluasi keamanan dan pengembangan jaringan.
Standar Minimal	Mencakup informasi tentang perangkat dan alokasi IP
Kuantitas	1 (satu) dokumen menjadi tanggungjawab Petugas Komunikasi.
Ketentuan Khusus	• Segmentasi/pemisahan jaringan yang digunakan untuk dinas/kantor dan layanan publik (misalnya akses poin internet, komputer layanan konsuler dan layanan publik yang lain). • Terdokumentasi dengan baik setiap perubahan dan penambahan perangkat disertai keterangan waktu *update.*

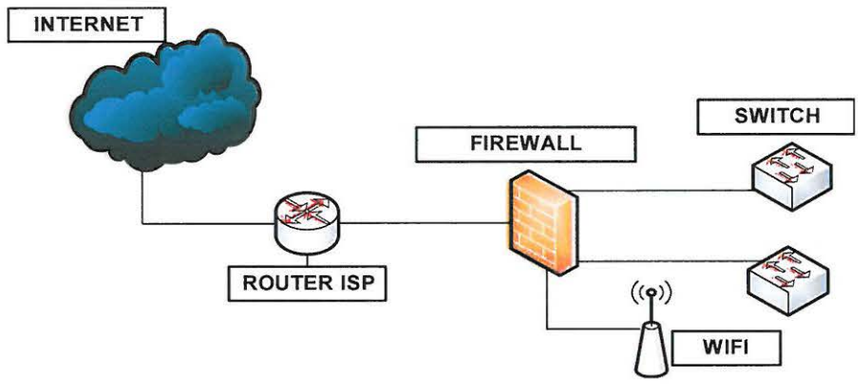


Standar topologi

Firewall	
Keterangan	*Firewall* digunakan sebagai kontrol pengamanan untuk membatasi aplikasi, port, dan paket-paket data yang tidak diijinkan keluar/masuk ke jaringan.
Standar Minimal	• Memiliki fitur standar *Stateful packet inspection* (SPI) dan *setting policy* (*firewall rules*). • Memiliki fitur pengelolaan MAC-*based access control*, IP/MAC *binding*, dan *wireless profiles*. • Dapat Static URL *blocking, keyword blocking, approved* URL • HTTPS, *username/password*. • *Port-based* RADIUS *authentication (Extensible Authentication Protocol* [EAP] MD5, *Protected* EAP [PEAP]).
Kuantitas	1 (satu)
Ketentuan Khusus	• Diletakkan pada rak jaringan • Dikelola oleh Petugas Komunikasi



contoh perangkat firewall



Penempatan firewall

Switch dan *Router* (akses poin)	
Keterangan	Router berfungsi untuk menghubungkan jaringan satu dengan lain dan membagi alamat IP, sedangkan switch digunakan untuk menghubungkan perangkat-perangkat komputer sehingga membentuk LAN.
Standar Minimal	• *Manageable* (dapat dikelola). • Memiliki fitur pengamanan (enkripsi) minimal WPA2-PSK untuk router Wifi. • Memiliki fitur ACL (*access control list*).
Kuantitas	Sesuai kebutuhan
Ketentuan Khusus	• Jika menggunakan perangkat dari vendor perlu diketahui spesifikasi teknis dan pengelolaannya (admin). • Mengganti *password* akses poin router Wifi secara periodik. • Diletakkan pada rak jaringan • Dikelola oleh unit komunikasi.



perangkat router wifi

PABX	
Keterangan	PABX digunakan untuk mendistribusikan panggilan dari/ke luar, serta membuat jaringan telepon internal.
Standar Minimal	• Digital/IP PABX (teknologi yang berlaku saat ini sesuai kebutuhan Perwakilan) • *Manageable* (dapat dikelola). • Mempunyai fitur manajemen pengamanan.
Kuantitas	1 (satu) sesuai kebutuhan
Ketentuan Khusus	• Dikelola oleh unit komunikasi. • Jika PABX disediakan oleh pengelola gedung/vendor, dokumentasi/pengelolaan dan pemeliharaan jaringan disupervisi oleh petugas perwakilan yang ditunjuk.



PABX

Rak Perangkat Jaringan (*Network Rack*)	
Keterangan	Rak perangkat jaringan digunakan untuk menyimpan perangkat jaringan seperti *router/switch, firewall*, server dan lain-lain untuk memudahkan pemeliharaan jaringan.
Standar Minimal	• *Wallmount Rack*/ rak yang diletakkan pada dinding atau; • *Close Rack/ Standing Rack* seperti lemari, lebar 19 inchi. • Minimal 4U atau sesuai kebutuhan jaringan Perwakilan. • Memiliki kunci pengaman. • Menggunakan kabel RG 45 sesuai standar.
Kuantitas	Sesuai Kebutuhan
Ketentuan Khusus	• Ditempatkan di ruang khusus/bagian ruangan yang tidak mudah diakses oleh orang yang tidak berwenang.

	• Suhu ruangan terjaga sesuai spesifikasi perangkat. • Pelabelan/penamaan/pemberian kode pada masing-masing kabel yang terhubung dengan perangkat dalam rak. • Pemasangan kabel harus memenuhi estetika dan keamanan secara fisik.



Rak jaringan 4U

Personal Computer/PC	
Keterangan	Perangkat komputer adalah peralatan yang digunakan oleh *user* langsung untuk komunikasi dan mengolah informasi perkantoran.
Standar Minimal	• Spesifikasi sesuai kebutuhan aplikasi yang dibutuhkan. • Minimal *dual core processor* 3,2 GHZ, RAM 4 GB, HD 320 GB, VGA 2 GB. • LAN card; konektor RJ-45, support BUS 32 bit, 1,000 mbps full duplex. • DVD/RW room combo 24x DVD 8x. • Monitor LCD/LED 16 inc. • Operating System yang berlaku saat ini dan kompatibel dengan perangkat/peralatan yang diinstal.
Kuantitas	Sesuai Kebutuhan
Ketentuan Khusus	• Menggunakan UPS (*uninterruptible power supply*) untuk meminimalisasi kerusakan *hardware* karena listrik. • Menggunakan *operating system* (OS) *original*/asli dan ter-*update*. • Menggunakan antivirus resmi yang berlisensi. • Komputer untuk mengolah dokumen rahasia tidak terhubung dengan LAN/internet. • Pemeliharaan dimonitor oleh personel terkait di bidang teknologi informasi.

E. STANDAR PENGAMANAN PERSONEL

Tanda Pengenal	
Keterangan	Tanda pengenal dipakai untuk mengidentifikasi keberadaan setiap individu yang berada di lingkungan Kementerian dan/atau Perwakilan.
Standar Minimal	Pembedaan warna dan *design* untuk masing-masing kategori.
Kuantitas	• ID untuk tamu • ID untuk personel
Ketentuan Khusus	• Tamu yang akan masuk harus diidentifikasi maksud dan tujuannya oleh petugas pos pengamanan dan/atau resepsionis. • Tamu diharuskan untuk meninggalkan ID pribadi untuk ditukar dengan ID tamu. • Tamu harus mengisi buku tamu.

Buku Tamu	
Keterangan	Pencatatan pada buku tamu diperlukan untuk melakukan pengawasan arus masuk dan keluar orang ke premis Kementerian dan Perwakilan yang bukan merupakan Personel Kementerian dan Perwakilan.
Standar Minimal	Minimal mencatat: • Nama tamu • Asal instansi / alamat • Keperluan • Jam masuk • Jam keluar
Kuantitas	Minimal 1 (satu) buah di pos pengamanan atau di meja resepsionis
Ketentuan Khusus	Buku tamu perlu dicek secara berkala.

Daftar Nomor Telepon Darurat	
Keterangan	Daftar ini diperlukan agar dalam keadaan tertentu, setiap Personel Kementerian dan Perwakilan dapat menghubungi aparat terkait ketika terjadi insiden keamanan yang membutuhkan bantuan dalam waktu yang cepat.
Standar Minimal	Data berupa: • *Contact person* dan nama instansi • Nomor telepon

	• Alamat instansi
Kuantitas	• Diberikan kepada seluruh Personel. • Ditempel di Pos Pengamanan.
Ketentuan Khusus	Memuat instansi-instansi antara lain: • Kantor Polisi lokal/nasional • Pemadam Kebakaran • Rumah sakit/*Ambulance* • Unit di Kementerian Luar Negeri setempat yang berhubungan langsung dengan pengamanan Perwakilan asing (untuk Perwakilan)

Contact list seluruh Tim Koordinasi Pengamanan Perwakilan RI	
Keterangan	Daftar ini mencatat kontak seluruh Tim Pengamanan Perwakilan RI agar setiap saat seluruh personel Perwakilan RI dapat melaporkan kejadian yang terkait dengan keamanan baik yang bersifat individu atau dalam lingkup institusi.
Standar Minimal	Memuat catatan: • Nama pejabat • Posisi dalam Tim • Nomor telepon yang dapat dihubungi setiap saat • Alamat tinggal
Kuantitas	Dimiliki oleh setiap personel Perwakilan RI
Ketentuan Khusus	-

MENTERI LUAR NEGERI
REPUBLIK INDONESIA,

ttd.

RETNO L.P. MARSUDI

LAMPIRAN III
PERATURAN MENTERI LUAR NEGERI
REPUBLIK INDONESIA
NOMOR 8 TAHUN 2019
TENTANG
PENGAMANAN KEMENTERIAN LUAR NEGERI DAN PERWAKILAN REPUBLIK INDONESIA

PEDOMAN PENYELENGGARAAN TANGGAP DARURAT

A. INDIKATOR PENETAPAN KONDISI DARURAT

Kementerian dan Perwakilan untuk mengantisipasi kondisi darurat harus menetapkan indikator-indikator yang dapat digunakan untuk menetapkan setiap tingkatan kesiagaan yang disesuaikan dengan karakteristik lingkungan setempat, baik karena bencana alam, krisis politik, maupun konflik bersenjata.

Tingkatan kesiagaan dari rendah ke tinggi dengan indikator sebagai berikut:

a. Siaga 3
   1) kondisi keamanan mulai memburuk;
   2) adanya kerusuhan di berbagai tempat secara meluas;
   3) aparat keamanan melakukan pemusatan kekuatan secara terbatas khususnya pada berbagai obyek vital;
   4) adanya antrian bahan pokok namun belum terdapat kelangkaan
   5) terganggunya sarana komunikasi; dan/atau
   6) perwakilan dan personel perwakilan asing menjadi sasaran tindakan kekerasan atau kejahatan.

b. Siaga 2
   1) situasi keamanan semakin memburuk;
   2) kebutuhan pokok mulai langka;
   3) adanya pembatasan dalam pergerakan;
   4) pengerahan pasukan militer di seluruh titik strategis negara akreditasi; dan/atau
   5) orang asing dijadikan target serangan oleh kelompok tertentu.

c. Siaga 1
   1) situasi dan kondisi keamanan memburuk sehingga dapat menyebabkan korban jiwa dalam jumlah besar dan sporadis;
   2) pemerintah dan aparat keamanan tidak dapat mengendalikan situasi secara efektif;

3) kebutuhan pokok sulit didapat (seperti: makanan, air bersih, dan bahan bakar); dan/atau
4) jalur transportasi utama terputus.

B. STRATEGI PENGAMANAN KEMENTERIAN DAN PERWAKILAN DALAM KONDISI STATUS DARURAT

Siaga 3

a. membentuk satuan tugas dan posko pengamanan;
b. memantau setiap perkembangan yang terjadi;
c. melakukan penilaian secara terus menerus terhadap kondisi objektif di lapangan dan melaporkannya kepada Komite Pengamanan secara berkala dan insidentil;
d. memastikan sistem pengamanan kementerian dan perwakilan berjalan dengan rutin;
e. melakukan pendekatan terhadap berbagai pemangku kepentingan di negara setempat; dan
f. memastikan keselamatan keluarga dengan membatasi dan memantau setiap pergerakannya ke luar dari tempat tinggal.

Siaga 2

a. memastikan ketersediaan kebutuhan pokok (seperti: makanan, air bersih, dan bahan bakar) di dalam Kementerian atau Perwakilan paling sedikit untuk 1 (satu) minggu ke depan;
b. membatasi kegiatan Personel dan keluarganya ke luar rumah/*compound*/kantor yang tidak terlalu mendesak. Apabila diharuskan untuk bertugas keluar dari premis Kementerian atau Perwakilan, setiap pergerakannya harus dimonitor dan terlaporkan kepada Komite Pengamanan atau Tim Pengamanan;
c. menginstruksikan agar setiap Personel selalu membawa tanda pengenal dan alat komunikasi;
d. merelokasi keluarga Personel ke tempat yang lebih aman;
e. menyiapkan dan mengumpulkan dokumen rahasia/sensitif (digital dan print) untuk persiapan dihancurkan;
f. melakukan penilaian secara terus menerus terhadap kondisi objektif di lapangan dan melaporkannya kepada Komite Pengamanan secara berkala dan insidentil;
g. memastikan gerbang dan pintu keluar atau masuk orang dan barang dalam keadaan terkontrol dan aman;
h. menentukan alur dan jalur evakuasi WNI/Personel Perwakilan; dan
i. meningkatkan koordinasi dengan Aparat Keamanan setempat untuk penyiapan pergerakan evakuasi.

Siaga 1

a. memastikan ketersediaan kebutuhan pokok (seperti: makanan, air bersih, dan bahan bakar) di dalam Kementerian atau Perwakilan paling sedikit untuk 1 (satu) bulan ke depan;
b. memberikan penilaian secara terus menerus terhadap kondisi obyektif di lapangan dan melaporkannya kepada Komite Pengamanan secara berkala dan insidentil, khususnya yang mengharuskan pelaksanaan evakuasi Warga Negara Indonesia dan Personel Perwakilan;
c. meminta arahan Pusat untuk pelaksanaan evakuasi, termasuk cara-cara dan waktu pelaksanaannya;
d. mengurangi pejabat dan personel (*essential*);
e. menghancurkan dokumen rahasia/sensitif (digital dan cetak);
f. menunjuk Personel untuk menjaga aset negara yang tertinggal di kantor;
g. memastikan gerbang Perwakilan dan pintu keluar/masuk orang dan barang terkontrol dan aman; dan
h. mengikuti arahan Komite Pengamanan dalam pelaksanan evakuasi.

MENTERI LUAR NEGERI
REPUBLIK INDONESIA,

ttd.

RETNO L.P. MARSUDI