ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

IMS
GOOD JOURNALISM | BETTER SOCIETIES

Funded by
the European Union

Panduan Membuat SOP Keamanan Digital Perusahaan Media



Panduan Membuat SOP Keamanan Digital Perusahaan Media

Penulis:
Sasmito
Adib Muttaqin Asfar

***Reviewer*:**
Arif Kurniawan

Penata Isi dan Perancang Sampul:
Krisna Sahwono

Januari 2025

Aliansi Jurnalis Independen (AJI) Indonesia
Jalan Kembang Raya No. 6, Kwitang, Senen
Jakarta Pusat 10420

Telp 021-3151214, Fax 3151261
Email: sekretariat@ajindonesia.or.id
Web: www.aji.or.id

Didukung oleh:

IMS
GOOD JOURNALISM | BETTER SOCIETIES

Funded by
the European Union

Daftar Isi

Kata Pengantar 4

BAB I. Pendahuluan 7

BAB II. Jenis-jenis Serangan Digital 10

BAB III. Pengertian SOP 14

BAB IV. Tahapan Penyusunan SOP 15

BAB V. Komponen SOP Keamanan Digital Perusahaan Media 20

BAB VI. Mekanisme Pencegahan dan Mekanisme Penanganan 24

BAB VII. Mekanisme Penanganan 44

BAB VIII. Panduan Keamanan Digital Organisasi Lain 56

BAB IX. Kontak Darurat 57

Kata Pengantar

Bukan Pilihan Tapi Kebutuhan

Dalam era digital yang semakin kompleks, keamanan digital bagi perusahaan media bukan lagi sekadar pilihan, melainkan kebutuhan mendesak.

Media berperan sebagai pilar keempat demokrasi, mengungkap kebenaran, dan menyajikan informasi yang akurat bagi publik. Peran yang semakin strategis membuat perusahaan media juga menjadi sasaran berbagai ancaman digital, mulai dari peretasan, serangan siber, hingga penyadapan komunikasi. Akibatnya? Ada dampak domino untuk media yang kritis dan independen.

Dalam beberapa tahun terakhir, serangan terhadap perusahaan media di Indonesia meningkat drastis, baik dari aktor negara, kelompok kriminal, maupun individu yang memiliki kepentingan tertentu.

Tanpa sistem keamanan digital yang kuat, media menghadapi berbagai risiko serius. Salah satunya adalah gangguan operasional, di mana serangan ransomware atau peretasan sistem dapat melumpuhkan aktivitas redaksi dan menghambat produksi berita.

Selain ancaman langsung terhadap perusahaan media, disinformasi dan manipulasi data juga menjadi tantangan besar. Dalam dunia yang semakin dipenuhi hoaks dan propaganda digital, kepercayaan publik terhadap media dapat runtuh jika ada celah keamanan yang memungkinkan pihak luar mengubah atau menyusupkan informasi palsu ke dalam berita.

Keamanan digital bukan hanya soal melindungi sistem internal media, tetapi juga memastikan bahwa informasi yang disampaikan kepada publik tetap dapat dipercaya dan tidak dimanipulasi oleh pihak yang berkepentingan.

Studi yang dilakukan oleh Pemantau Regulasi dan Regulator Media (PR2Media) bersama Aliansi Jurnalis Independen (AJI) pada 29 Mei–19 Juni 2024 terhadap 116 perusahaan media mengungkap bahwa tingkat keamanan digital perusahaan media siber masih tergolong rendah. Hal ini tercermin dari Indeks Keamanan Digital yang hanya mencapai 19,71 dari nilai maksimal 31.

PR2Media menggunakan lima indikator untuk menilai praktik pengamanan digital dalam perusahaan media. Dari riset tersebut hanya aspek keberadaan sumber daya khusus dalam teknologi informasi yang mendapatkan penilaian baik. Sementara itu, empat indikator lainnya—termasuk SOP, edukasi, audit keamanan, dan asesmen risiko—masih menunjukkan skor yang rendah atau tidak memadai, mengindikasikan perlunya peningkatan strategi keamanan digital di sektor media.

Riset ini yang akhirnya mendesak AJI Indonesia untuk menerbitkan Panduan Membuat SOP Keamanan Digital Perusahaan Media.

Panduan ini akan menuntun perusahaan media melakukan pengamanan digital digital perusahaan media, termasuk strategi perlindungan data, praktik keamanan untuk jurnalis, enkripsi komunikasi, mitigasi serangan siber, serta langkah-langkah yang bisa diambil untuk membangun ekosistem media yang lebih aman.

Dengan memahami tantangan yang ada dan menerapkan langkah-langkah perlindungan yang tepat, perusahaan media dapat terus menjalankan tugasnya dengan lebih aman dan efektif, tanpa harus takut akan ancaman digital yang semakin canggih.

AJI Indonesia berharap buku Panduan Membuat SOP Keamanan Digital Perusahaan Media dapat menjadi panduan praktis bagi pemimpin redaksi,

manajer IT, jurnalis, dan seluruh ekosistem media dalam membangun sistem keamanan digital yang lebih tangguh.

Perlu ditekankan bahwa keamanan digital bukan hanya tanggung jawab satu individu atau satu departemen dalam media, tetapi merupakan komitmen bersama untuk menjaga kebebasan pers dan memastikan bahwa media tetap menjadi sumber informasi yang kredibel dan dapat diandalkan.

AJI mengucapkan terima kasih untuk Sasmito dan Adib Muttaqin Asfar yang sudah menulis buku yang maha penting ini. Harapannya Panduan Membuat SOP Keamanan Digital Perusahaan Media ini dapat menjadi awalan untuk media yang masih bingung bagaimana harus memulai.

Semoga Panduan Membuat SOP Keamanan Digital Perusahaan Media ini dapat menjadi langkah awal menuju ekosistem media yang lebih resilien di era digital.

Nany Afrida
Ketua AJI Indonesia

BAB I
Pendahuluan

Survei yang dilakukan Pemantau Regulasi dan Regulator Media (PR2Media) dan Aliansi Jurnalis Independen (AJI) pada 29 Mei-19 Juni 2024 terhadap 116 perusahaan media menemukan keamanan perusahaan media siber kurang baik.[1] Ini terlihat dari Indeks Keamanan Digital yang terlihat dari survei ini hanya 19,71 dari nilai maksimal 31. Nilai ini berdasarkan tiga aspek yaitu pengalaman terkait serangan digital, praktik pengamanan digital, dan persepsi terhadap keamanan digital. Satu dari tiga aspek yang menjadi catatan yaitu nilai aspek praktik pengamanan digital (5,03) yang masih jauh dari nilai maksimal (11). Sementara untuk pengalaman terkait serangan digital relatif cukup baik dan persepsi terhadap keamanan digital nilainya baik.

Terdapat lima indikator yang digunakan PR2Media untuk menilai aspek praktik pengamanan digital yaitu keberadaan standard operating procedure (SOP) atau prosedur operasional standar, edukasi dan pelatihan keamanan bagi pekerja media, keberadaan sumber daya khusus dalam teknologi informasi untuk mencegah serangan digital, pelaksanaan audit keamanan

[1] https://aji.or.id/data/laporan-riset-keamanan-digital-perusahaan-media-di-indonesia

digital terhadap perusahaan, dan pelaksanaan asesmen risiko keamanan digital terhadap karyawan dan kontributor. Dari lima indikator tersebut, hanya keberadaan sumber daya khusus yang terbilang baik. Sedangkan empat indikator lainnya menunjukkan nilai yang kurang baik atau tidak baik.

PR2Media juga menggelar diskusi kelompok terarah secara daring bersama 13 orang yang dipilih dari responden survei pada 9 Juli 2024. Diskusi ini bertujuan untuk memperdalam temuan survei tentang keamanan digital perusahaan media. Hasil diskusi ini memberi gambaran yang lebih utuh terkait praktik pengamanan digital. Misal terkait temuan sebagian besar responden menyatakan memiliki SOP keamanan digital. Dalam diskusi terkonfirmasi, SOP tersebut hanya sebatas pada panduan internal di tim teknologi informasi, tidak selalu tertulis, dan tidak menyentuh aset digital terkait kerja jurnalistik perusahaan seperti akun aplikasi digital yang dipakai oleh jurnalis. Begitu pula terkait temuan edukasi dan pelatihan, diskusi tersebut mengungkap bahwa kegiatan tersebut tidak semata diberikan oleh perusahaan media. Namun, kegiatan tersebut juga diberikan pihak eksternal seperti AJI Indonesia, IREX, dan SAFEnet.

Kedua, terkait aspek pengalaman terkait serangan digital yang relatif baik. Riset ini juga menemukan bahwa 71,6 persen dari 116 responden pernah mengalami setidaknya satu dari sembilan jenis serangan digital yang ditanyakan. Tiga jenis serangan yang sering dialami perusahaan media yaitu serangan *buzzer*/pendengung, serangan terhadap situs web, dan laporan palsu/tidak berdasar terkait akun media sosial.

Dari sembilan jenis serangan digital tersebut, jenis serangan yang paling sering dialami oleh perusahaan media adalah "serangan buzzer/pendengung" (nilai 3,07) dan "serangan terhadap situs web" (nilai 3,09). Sementara itu, jenis serangan yang paling jarang dialami adalah "ransomware" (nilai 3,88) dan "intersepsi/penyadapan" (nilai 3,87).

Sedangkan menurut catatan Aliansi Jurnalis Independen (AJI) terdapat 14 serangan digital sepanjang 2023. Jenis serangan paling banyak yaitu

peretasan (7 kasus), disusul penangguhan website/akun media sosial (3 kasus), serangan terhadap situs web (3 kasus), doxing (1 kasus).

Atas data-data tersebut, perusahaan media penting untuk memperkuat praktik pengamanan digital dengan lebih baik. Untuk itu, perlu tahapan awal yaitu adanya SOP keamanan digital yang bisa dijadikan panduan bersama bagi semua pekerja di perusahaan media, tidak hanya sebatas pada panduan internal di tim teknologi informasi.

BAB II
Jenis-jenis Serangan Digital

Berikut ini jenis serangan digital yang diidentifikasi PR2Media dan AJI dalam riset "Keamanan Digital Perusahaan Media di Indonesia" 2024:

a. Malware

Akronim dari *malicious software* (perangkat lunak berbahaya) adalah program atau file yang berbahaya bagi pengguna komputer atau ponsel. Jenis *malware* dapat mencakup virus, *worm*, *trojan horse*, dan *spyware*. Program jahat ini dapat melakukan berbagai fungsi berbeda seperti mencuri, mengenkripsi, atau menghapus data, mengubah atau membajak fungsi komputasi inti dan memantau aktivitas komputer atau ponsel pengguna tanpa izin mereka.

b. Doxing

Doxing adalah serangan digital yang dilakukan seseorang atau kelompok dengan sengaja mengumpulkan dan memublikasikan informasi pribadi orang lain secara online tanpa izin, biasanya dengan niat jahat atau untuk merugikan korban. Istilah "*doxing*" berasal dari kata "*documents*" (dox), yang merujuk pada dokumen atau data pribadi yang diekspos kepada publik.

Pelaku *doxing* biasanya memiliki berbagai tujuan, seperti:

- Membalas dendam atau mengintimidasi: agar korban merasa tidak aman.
- Merusak reputasi: menyebarkan informasi yang memalukan untuk mencoreng nama baik seseorang.
- Mendorong serangan lain: membuka informasi agar orang lain bisa melakukan ancaman, intimidasi, atau kekerasan.
- Aktivisme atau hacktivisme[2]: terkadang digunakan untuk membocorkan informasi tentang pihak yang dianggap "berbahaya" secara sosial atau politik.

c. Intersepsi atau penyadapan

Intersepsi atau penyadapan adalah tindakan mencuri atau menyadap komunikasi digital tanpa izin, yang dilakukan melalui metode *hacking* seperti *Man-in-the-Middle* (MITM)[3], *packet sniffing*, atau aplikasi berbahaya seperti aplikasi mata-mata *spyware* dan aplikasi perekam keyboard keylogger. Penyadapan menjadi serangan digital karena melanggar privasi, mengeksploitasi data sensitif, mengancam keamanan nasional, serta sering digunakan untuk aktivitas kriminal seperti pemerasan atau penipuan.

d. Social engineering

Social engineering adalah teknik manipulasi psikologis yang digunakan oleh pelaku kejahatan untuk mengelabui seseorang agar memberikan informasi sensitif atau melakukan tindakan tertentu, seperti membocorkan kata sandi, data pribadi, atau akses ke sistem. Metode ini sering me-

[2] Hacktivisme adalah bentuk serangan siber yang dilakukan oleh para peretas (*hacker*) dengan tujuan politis atau sosial. Mereka menggunakan keterampilan teknis untuk mengakses, merusak, atau mengganggu situs web, sistem, atau jaringan sebagai cara untuk menyuarakan protes, mempengaruhi opini publik, atau melawan kebijakan yang dianggap tidak adil. Hacktivisme bisa berupa serangan DDoS (menyebabkan gangguan akses ke situs), *defacing* (mengubah tampilan situs web), atau membocorkan informasi yang sensitif untuk mengekspos pelanggaran. Tujuan utamanya adalah untuk memengaruhi perubahan sosial atau politik melalui kekuatan teknologi.

[3] Serangan *Man-in-the-Middle* (MITM) adalah jenis serangan siber yang dilakukan penyerang secara diam-diam menyusup di antara dua pihak yang sedang berkomunikasi untuk mencuri atau memanipulasi data mereka. Dalam serangan ini, penyerang dapat memonitor, mengubah, atau bahkan mengarahkan ulang pesan tanpa sepengetahuan korban.

manfaatkan kepercayaan, rasa takut, atau urgensi melalui taktik seperti *phishing*, *pretexting*, *baiting*, atau *vishing* (*voice phishing*). *Social engineering* berbahaya karena memanfaatkan kelemahan manusia alih-alih celah teknis, membuatnya sulit diantisipasi.

e. Phishing

Phishing adalah serangan siber yang dilakukan pelaku dengan menyamar sebagai entitas atau individu tepercaya untuk menipu korban agar memberikan informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi. Serangan ini biasanya dilakukan melalui *email*, pesan teks, atau situs web palsu yang tampak sah untuk memancing korban masuk perangkap.

f. Serangan terhadap website

Upaya tidak sah untuk mendapatkan akses ke situs web dengan tujuan mengubah, mencuri, memasukkan atau memublikasikan konten berbahaya. Contohnya yaitu mengganti tampilan visual atau konten website (defacement) dan DDoS (Distributed Denial-of-Service).

g. Perampasan perangkat digital

Perampasan perangkat fisik digital adalah tindakan mengambil secara paksa atau mencuri perangkat digital seperti ponsel, laptop, atau perangkat lainnya dengan tujuan mengakses data sensitif, menyabotase, atau mengeksploitasi informasi yang ada di dalamnya. Ancaman ini tidak hanya melibatkan kehilangan perangkat fisik, tetapi juga risiko keamanan digital jika perangkat tidak terlindungi dengan kata sandi, enkripsi, atau fitur pelacakan.

h. Serangan digital berbasis gender

Serangan digital berbasis gender adalah jenis serangan siber yang menargetkan individu berdasarkan identitas gender mereka, dengan tujuan untuk merendahkan, mengintimidasi, atau mengendalikan korban. Serangan ini dapat berupa pelecehan seksual, intimidasi verbal, perundungan *online*, penyebaran gambar atau video pribadi, hingga *doxing* (penyebaran informasi pribadi). Korban, terutama

perempuan dan kelompok gender minoritas, sering menjadi sasaran karena ketidaksetaraan gender dan stereotip sosial. Serangan ini dapat menimbulkan dampak psikologis yang berat, serta mengancam hak privasi dan keselamatan individu.

i. Ancaman dan intimidasi di ranah digital

Ancaman merupakan bentuk komunikasi yang disampaikan orang atau lembaga dengan tujuan menimbulkan kerugian pada orang atau lembaga lain. Sedangkan intimidasi merupakan tindakan menakut-nakuti yang dilakukan orang atau lembaga untuk memaksa orang atau lembaga lain berbuat atau tidak berbuat sesuatu.

Ancaman dan intimidasi tersebut biasanya disampaikan secara daring agar perusahaan media atau awak menghentikan liputan yang merugikan pihak tertentu.

BAB III
Pengertian SOP

Secara sederhana, prosedur operasional standar atau lebih dikenal SOP Keamanan Digital Perusahaan Media dapat diartikan sebagai dokumen resmi perusahaan media yang menjelaskan langkah-langkah bagi semua orang di perusahaan media untuk mencegah dan menangani serangan digital.

Maksud semua orang berarti SOP ini berlaku dari level paling tinggi (jajaran redaksi) hingga level paling bawah pekerja media di perusahaan. Sebab dalam riset AJI dan PR2Media, SOP Keamanan Digital biasanya hanya sebatas panduan internal di tim teknologi informasi.

BAB IV
Tahapan Penyusunan SOP

SOP yang baik adalah SOP yang disusun secara partisipatif melibatkan semua orang di perusahaan media. Sebab, keamanan digital perusahaan media merupakan satu kesatuan tindakan dari semua pihak yang saling berkaitan untuk terwujudnya keamanan digital. Karena itu, penting bagi semua orang dari level paling bawah hingga tinggi terlibat dalam penyusunan SOP Keamanan Digital Perusahaan Media.

Berikut ini sejumlah langkah penyusunan SOP Keamanan Digital Perusahaan Media yang dapat diadopsi perusahaan media:

1. **Mulai dari audit keamanan digital:**
   Audit keamanan digital penting untuk mengetahui risiko, ancaman, kapasitas organisasi, dan perilaku orang di perusahaan media yang berkaitan dengan keamanan digital. Audit keamanan digital bisa dilakukan secara mandiri atau dengan bantuan pihak eksternal yang berpengalaman melakukan audit.

   Bagi perusahaan media yang ingin melakukan secara mandiri dapat mempelajari "Panduan Audit Keamanan Digital untuk OMS" yang dibuat oleh SAFEnet.[4]

[4] Panduan bisa diakses melalui link ini: https://safenet.or.id/id/2024/09/panduan-audit-keamanan-digital-untuk-oms/

Panduan ini menggunakan Security Auditing Framework and Evaluation Template for Advocacy Groups (SAFETAG) sebagai referensi utama, terutama dari sisi konten dan struktur pelaksanaannya. Namun, SAFEnet juga mengadaptasi pengalaman mereka dalam melakukan audit selama empat tahun terakhir.

2. Pembentukan tim penyusun SOP Keamanan Digital

Pemimpin perusahaan media dapat membentuk tim penyusun "SOP Keamanan Digital Perusahaan Media" untuk menyusun draf awalan SOP. Tim bisa terdiri dari berbagai departemen antara lain departemen teknologi informasi, redaksi, sekretariat, dan legal. Anggota tim yang beragam membantu penyusunan draf SOP bisa lebih matang karena mendapat masukan dari berbagai departemen.

Pemimpin perusahaan juga dapat menunjuk koordinator dan anggota penyusunan "SOP Keamanan Digital Perusahaan Media" melalui surat keputusan (SK). Dokumen SK tersebut bisa menjadi legitimasi bagi tim penyusun bekerja, termasuk juga dukungan anggaran yang dibutuhkan.

3. Buat tahapan penyusunan SOP

Tim penyusunan "SOP Keamanan Digital Perusahaan Media" dapat memulai kerja dengan menggelar rapat pertama secara bersama. Koordinator tim perlu menjelaskan kepada semua anggota tim terkait urgensi dan tujuan dalam penyusunan SOP Keamanan Digital. Ini supaya semua anggota tim memiliki persepsi yang sama tentang pentingnya SOP Keamanan Digital Perusahaan Media.

Selanjutnya, koordinator bisa membahas secara partisipatif tentang rencana kerja, tahapan dan jadwal kerja penyusunan SOP. Pembahasan yang partisipatif akan membuat rencana kerja tersebut berjalan lebih realistis dan sesuai dengan kemampuan anggota tim. Dengan demikian, perkembangan kerja bisa lebih terukur dan selesai dengan jadwal yang diharapkan.

4. Pelajari hasil audit keamanan digital

Tim penyusun SOP Keamanan Digital bisa mempelajari hasil audit keamanan digital terlebih dahulu, sebelum menyusun draf SOP. Hal ini penting untuk mengetahui kelemahan dan kelebihan perusahaan media terkait keamanan digital. Tim penyusun selanjutnya bisa merumuskan sejumlah langkah yang perlu dilakukan sehingga kelemahan tersebut bisa ditutup dalam SOP. Sekaligus untuk memperkecil risiko dan ancaman perusahaan media dari serangan digital.

Hasil audit tersebut juga bisa jadi alat ukur bagi tim penyusun untuk melihat kapasitas organisasi dan perilaku orang di perusahaan media. Karena itu, tim penyusun bisa membuat usulan langkah-langkah yang bisa dilakukan dalam SOP sesuai dengan kemampuan perusahaan. Termasuk usulan budaya organisasi jika terdapat perilaku manusia yang membahayakan keamanan digital perusahaan media.

5. Penyusunan draf awal SOP Keamanan Digital

SOP Keamanan Digital Perusahaan Media yang baik setidaknya terdiri dari sejumlah komponen yang bisa dipahami semua orang di perusahaan media. Antara lain yaitu latar belakang, tujuan, ruang lingkup, prinsip-prinsip, mekanisme pencegahan, mekanisme penanganan, mekanisme pengawasan dan evaluasi.

Tim penyusun juga bisa menambahkan komponen lain seperti istilah kunci, landasan hukum, dan referensi. Hal ini untuk memudahkan semua orang di perusahaan lebih memahami SOP. Sebab, SOP ini nantinya tidak hanya berlaku untuk tim internal teknologi informasi, melainkan semua orang dari level paling bawah hingga level tertinggi di perusahaan media.

6. Presentasikan draf awal SOP Keamanan Digital

Tim penyusun SOP Keamanan Digital Perusahaan Media perlu membagikan draf awal ke semua orang di perusahaan media untuk mendapatkan masukan dan tanggapan. Draf tersebut dapat dibagikan melalui saluran komunikasi yang aman, baik melalui email maupun

cetak. Selain itu, tim penyusun perlu mempresentasikan kepada semua departemen dan pimpinan yang ada di perusahaan media.

Presentasi tersebut dapat melengkapi masukan dan tanggapan, sekaligus memperkaya draf SOP secara langsung dari masing-masing departemen dan pimpinan perusahaan. Sekaligus mendiskusikan dengan pimpinan perusahaan jika terdapat komponen biaya dalam draf SOP yang akan dibuat. Semisal pembelian software resmi (bukan bajakan) dan antivirus bagi pekerja media.

7. Penyempurnaan draf SOP Keamanan Digital

Tim penyusun dapat menyempurnakan draf SOP Keamanan Digital Perusahaan Media dengan mempertimbangkan masukan seluruh pekerja media dari berbagai departemen dan pimpinan media. Tim juga perlu menyimulasikan draf tersebut kepada perwakilan pekerja media dan pimpinan sebelum menjadi draf akhir.

Baru kemudian setelah simulasi dan draf tersebut terbukti bisa dijalankan, maka tim penyusun bisa menyampaikan kepada pimpinan. Dengan demikian, tugas dari tim penyusun telah selesai dalam mempersiapkan draf SOP Keamanan Digital Perusahaan Media.

8. Pembuatan peraturan SOP Keamanan Digital

Pemimpin perusahaan bisa melanjutkan kerja tim penyusun dengan membuat “Surat Keputusan tentang SOP Keamanan Digital Perusahaan Media”. Hal ini supaya SOP memiliki legitimasi yang kuat karena dikeluarkan oleh pemimpin perusahaan dan bisa dipatuhi oleh semua orang yang ada di dalam perusahaan media.

9. Sosialisasi dan implementasi SOP Keamanan Digital

Peraturan tentang SOP Keamanan Digital perlu disosialisasikan kepada semua orang di perusahaan media sebelum diimplementasikan. Sosialisasi tersebut penting untuk menyamakan pandangan tentang regulasi baru yang dimiliki perusahaan media.

10. Pengawasan dan evaluasi

Perusahaan media perlu menunjuk pengawas dalam implementasi SOP Keamanan Digital Perusahaan Media agar berjalan sesuai dengan peraturan. Pengawas tersebut bisa berasal dari departemen SDM dan departemen teknologi informasi. Selain itu, pengawas juga perlu melakukan evaluasi terhadap implementasi SOP Keamanan Digital untuk perbaikan peraturan ke depan. Sebab, kekurangan SOP pada umumnya akan terlihat ketika peraturan ini sudah berjalan.

BAB V
Komponen SOP Keamanan Digital Perusahaan Media

SOP Keamanan Digital Perusahaan Media yang baik setidaknya terdiri dari sejumlah komponen yang bisa dipahami semua orang di perusahaan media. Antara lain yaitu latar belakang, tujuan, ruang lingkup, prinsip-prinsip, mekanisme pencegahan, mekanisme penanganan, mekanisme pengawasan dan evaluasi.

Tim penyusun juga bisa menambahkan komponen lain seperti istilah kunci, landasan hukum, dan referensi. Hal ini untuk memudahkan semua orang di perusahaan lebih memahami SOP. Sebab, SOP ini nantinya tidak hanya berlaku untuk tim internal teknologi informasi, melainkan semua orang dari level paling bawah hingga level tertinggi di perusahaan media.

Di bawah ini merupakan komponen SOP Keamanan Digital Perusahaan Media yang dapat diadopsi.

1. **Judul SOP**
   Judul SOP penting untuk memberikan penjelasan di awal kepada semua orang yang ada di dalam perusahaan. Semisal “SOP Keamanan Digital Perusahaan Media Kabar Batavia”.

2. **Latar belakang**
   Latar belakang berisi tentang alasan dan pertimbangan dari perusahaan

media membutuhkan SOP Keamanan Digital. Semisal berdasarkan audit keamanan digital diketahui terdapat ancaman serangan digital yang besar dan kurangnya kapasitas perusahaan dalam mencegah serangan digital. Atas dasar tersebut, perusahaan memandang perlu untuk membuat SOP Keamanan Digital Perusahaan Media.

3. Tujuan

Bagian ini menggambarkan tujuan yang ingin dicapai perusahaan media dengan pembuatan SOP Keamanan Digital Perusahaan Media. Semisal untuk memastikan keamanan data, sistem, karya jurnalistik dan konten media, dan informasi rahasia dari serangan digital.

4. Ruang lingkup

Ruang lingkup merupakan cakupan atau batasan dari aktivitas, proses, dan pembagian tugas dalam SOP. Contoh ruang lingkupnya mencakup sistem manajemen konten, data redaksi dan pengguna, karya jurnalistik, dan akses jaringan yang digunakan perusahaan media.

5. Prinsip-prinsip

Berikut prinsip-prinsip keamanan digital yang dapat diadopsi perusahaan media dalam pembuatan SOP Keamanan Digital Perusahaan Media:

A. Keamanan data dan konten: jaminan terhadap data dan konten perusahaan media baik dari akses yang tidak sah maupun serangan digital.
B. Keamanan data pengguna: perusahaan media perlu melindungi keamanan data pribadi pengguna sesuai dengan Undang-Undang Perlindungan Data Pribadi yang berlaku di Indonesia. Setidaknya antara lain tanggung jawab dan kepatuhan pada aturan pemrosesan data pribadi, memastikan keamanan pemrosesan data pribadi, melakukan pencatatan kegiatan pemrosesan data pribadi, dan kewajiban menjaga kerahasiaan data pribadi.[5]

[5] https://aji.or.id/system/files/2024-08/modul-pelindungan-data-pribadi.pdf

C. Kerahasiaan: data dan informasi merupakan aset penting bagi perusahaan media. Terutama dalam liputan-liputan investigasi sehingga perlu dijaga kerahasiaannya.
D. Akses kontrol: prinsip ini memastikan hanya orang yang memiliki otoritas dan berdasarkan kebutuhan tugas yang bisa mengakses sistem perusahaan.
E. Cadangan dan pemulihan: perusahaan media perlu membuat cadangan data dan konten secara berkala untuk mencegah kehilangan aset digital perusahaan karena serangan digital.
F. Ketersediaan: sumber daya manusia dan keuangan perlu tersedia untuk memastikan keamanan digital, pencegahan dan penanganan serangan digital dapat dilakukan perusahaan media.
G. Kerja sama/komitmen bersama: keamanan perusahaan media merupakan satu kesatuan tindakan dan perilaku dari semua orang di perusahaan.

6. Mekanisme Pencegahan

Mekanisme pencegahan terhadap serangan digital merupakan rangkaian tindakan yang dilakukan secara bersama-sama untuk terwujudnya keamanan digital di perusahaan media. Karena itu, penting bagi semua orang di perusahaan memiliki pemahaman yang sama tentang keamanan digital. Perusahaan bisa menggelar pelatihan dasar tentang keamanan digital untuk menyamakan pandangan pekerja dan pimpinan perusahaan media.

Selain itu, tindakan pencegahan dari serangan digital dapat dituangkan secara detail dalam SOP untuk menjadi pedoman bagi semua orang di perusahaan. Sejumlah tindakan pencegahan juga dapat diadopsi di bagian bawah buku ini.

7. Mekanisme Penanganan

Mekanisme penanganan merupakan rangkaian kegiatan yang dilakukan perusahaan media jika mendapatkan serangan digital. Penanganan tersebut dapat dilakukan orang tim internal maupun eksternal

perusahaan media. Semisal penanganan peretasan akun media sosial perusahaan media yang harus melibatkan perusahaan platform digital dalam penanganan.

8. Mekanisme pengawasan dan evaluasi

Setiap aktivitas digital harus tercatat secara transparan dan dapat dipertanggungjawabkan. Hal ini akan memudahkan perusahaan media melakukan evaluasi terhadap pelaksanaan SOP Keamanan Digital Perusahaan Media. Termasuk juga saat terjadi serangan digital, maka perusahaan media perlu mendokumentasikan serangan tersebut agar dapat menjadi bahan evaluasi bersama.

Namun yang tidak kalah penting adalah pengawasan terhadap implementasi SOP Keamanan Digital Perusahaan Media. Pimpinan perusahaan bisa menunjuk pengawas dari departemen SDM dan departemen teknologi informasi. Hasil evaluasi dan pengawasan ini bisa menjadi bahan untuk memperbaiki SOP Keamanan Digital Perusahaan Media. Apalagi di tengah perkembangan teknologi informasi yang berkembang secara eksponensial.

BAB VI
Mekanisme Pencegahan dan Mekanisme Penanganan

Sejumlah langkah di bawah ini dapat diadopsi perusahaan media dalam melakukan pencegahan dan penanganan serangan digital. Langkah ini juga dapat dimasukkan ke dalam SOP Keamanan Digital. Kendati demikian, potensi serangan digital setiap perusahaan media berbeda satu dengan lainnya. Karena itu, penting perusahaan media menyinkronkan potensi serangan digital yang paling utama berdasarkan audit digital dengan langkah pencegahan dan penanganan di SOP yang akan dibuat.

Langkah-langkah di bawah ini menggunakan bahasa teknis yang kemungkinan besar lebih mudah dipahami pekerja di departemen teknologi informasi. Namun demikian, kami berharap pekerja media di departemen lain maupun pimpinan perusahaan media bisa mendapatkan gambaran umum dari penjelasan di bawah ini. Kami juga menyarankan pekerja di departemen lain dan pimpinan perusahaan untuk berdiskusi dengan departemen teknologi informasi agar mendapatkan gambaran umum tentang langkah-langkah berikut ini.

A. Keamanan Jaringan di Kantor

Sebuah lembaga, termasuk perusahaan media dengan kantor fisik memiliki banyak pekerjaan yang mengharuskan banyak perangkat terhubung dalam jaringan. Perangkat itu antara lain komputer, printer, server, dan sebagainya yang digunakan khusus oleh para awak media.

Di sisi lain, kantor media juga memiliki ruang-ruang yang bisa diakses oleh publik seperti pengunjung atau para klien mereka. Ruang publik ini umumnya juga dilengkapi jaringan internet seperti WiFi dan fasilitas lain yang bisa diakses publik. Membuka ruang untuk publik, termasuk jaringan internet, berpotensi membuka celah keamanan bagi media tersebut. Karena itu, ada beberapa hal yang perlu diperhatikan dalam mengelola jaringan.

1. Kenali perangkat jaringan di kantor
   - Perangkat itu antara lain *router, switch, network printer, access point* Wi-Fi, NAS (LAN *file storage/file sharing*), *network projector* (yang tersambung melalui Wi-Fi), *modem broadband*, *smart TV*, mikrotik, jaringan internet yang terhubung dalam domain, kamera CCTV, dan lainnya.
   - Pastikan perangkat-perangkat tersebut terhubung jaringan yang aman dan tidak diakses oleh publik/orang luar.
   - Pastikan perangkat-perangkat tersebut berada di tempat yang aman dan tidak terekspos ke publik/orang luar.

2. Kenali perangkat nonjaringan
   Beberapa perangkat yang tidak terhubung jaringan bisa jadi memiliki media penyimpanan seperti mesin foto kopi, *hard disk* eksternal, dan sebagainya.

3. Pemisahan jaringan
   - Jika memungkinkan, pisahkan jaringan untuk koneksi internet dan perangkat-perangkat untuk pekerjaan awak media tersebut terpisah dari jaringan untuk publik.

- Akses jaringan untuk tamu seperti WiFi untuk publik harus terpisah dari jaringan untuk internal. Hal ini penting untuk mencegah jaringan untuk internal dimasuki orang luar.
- Pengaturan *service set identifier* (SSID) atau nama yang digunakan untuk membedakan jaringan Wi-Fi satu sama lain. SSID biasanya dibagi menjadi dua jenis, yakni hidden SSID dan public SSID. Pada *hidden* SSID, pengelola WiFi dapat menyembunyikan nama SSID sehingga hanya orang-orang tertentu yang dapat melihat dan menggunakan jaringan tersebut. Sedangkan publik di luar lembaga hanya bisa melihat *public* SSID yang bisa diakses tanpa kunci, atau Wi-Fi *protected access* (WPA) yang penggunanya hanya perlu memasukkan *password*.
- Jika tidak memungkinkan pemisahan, sebaiknya tidak ada jaringan yang bisa diakses orang luar.

4. Manajemen akses WiFi
    - Jaringan WiFi sebaiknya disembunyikan agar tidak mudah ditangkap dan dikenali pihak dari luar perusahaan media, termasuk dari lingkungan di sekitar bangunan kantor.
    - Akses ke WiFI (*username* dan *password*) tidak dipublikasikan untuk umum, tetapi hanya diberikan untuk perangkat-perangkat (*desktop* maupun *mobile*) yang telah terdaftar.
    - Setiap perangkat yang terhubung dengan jaringan termasuk WiFi harus dikenali. Karena itu, nama perangkat perlu diganti dari nama bawaan pabrikan pembuatnya. Misalnya nama laptop atau *smartphone* diubah dari "DESKTOP ****" menjadi nama unik lain yang bisa dikenali oleh admin jaringan.
    - Kenali risiko yang berpotensi terjadi jika publik bisa mengakses jaringan internet kantor. Seseorang yang memiliki akses terhadap jaringan internet tersebut bisa mendapatkan informasi setidaknya *internet protocol* (IP) *address*. IP *address* adalah identitas perangkat yang terhubung ke jaringan internet atau jaringan. Jika IP *address* perangkat kita diketahui publik, ini menjadi celah yang bisa dimanfaatkan pihak luar melakukan serangan seperti mengirim *malware*, melacak lokasi, atau melakukan akses ilegal.

5. Manajemen Local Area Network (LAN)
   Jika kantor media menggunakan LAN, pastikan hanya bisa diakses oleh orang-orang internal dengan perangkat tertentu. Jika semua perangkat *desktop* (termasuk milik tamu) bisa terhubung dengan LAN, risiko keamanan semakin besar.

6. Pengelola jaringan
   - Pertimbangkan orang internal/staf khusus menjadi pengelola jaringan kantor.
   - Jika jaringan LAN dan WiFi dikelola oleh pihak ketiga, pastikan pihak ketiga tersebut sudah dikenal, bisa dipercaya, dan latar belakangnya tidak terkait lembaga/orang yang berpotensi mengancam keamanan media.
   - Pastikan narahubung pihak ketiga tersebut bisa selalu dihubungi.

B. Keamanan Perangkat di Kantor

Ini menyangkut semua perangkat yang dimiliki oleh lembaga media dan awaknya, baik dalam bentuk perangkat keras, perangkat lunak, maupun akun-akun platform digital. Perangkat keras bisa berupa komputer, laptop, ponsel, *router*, *server*, dan sebagainya. Sedangkan perangkat lunak mencakup sistem operasi, program, dan aplikasi yang digunakan baik oleh perusahaan media maupun para awaknya. Akun-akun platform digital terdiri atas akun media sosial, aplikasi percakapan, surat elektronik, dan platform lain yang dimiliki media serta awak media secara pribadi.

Untuk memastikan keamanan aset-aset tersebut, pastikan:

1. Perangkat terhubung
   Pastikan setiap perangkat yang terhubung dengan jaringan baik *local area network* (LAN) maupun WiFi dikenali dan tidak ada perangkat asing yang tidak dikehendaki terhubung jaringan.

2. Komputer dan laptop
   - Identifikasi perangkat-perangkat yang selalu mobile atau bisa dibawa pulang (seperti laptop) dan perangkat yang selalu berada di kantor (seperti PC).

- Tempatkan perangkat seperti PC yang selalu berada di kantor, di ruang yang tidak bisa diakses oleh publik/tamu. Sedangkan perangkat seperti laptop yang *mobile* harus dikelola dengan aman oleh penggunanya.
- Gunakan sistem operasi/*operating system* (OS) yang berlisensi alias tidak bajakan. Penggunaan OS bajakan atau tanpa lisensi akan membuat celah keamanan yang tidak bisa dilindungi oleh pengembang OS sehingga rentan serangan virus dan *malware*. Alternatif lainnya adalah menggunakan OS *open source*, misalnya yang berbasis Linux seperti GNU/Linux, Ubuntu, dan lainnya.
- Gunakan hanya jaringan kantor yang tersedia (WiFi atau LAN) atau jaringan tepercaya lainnya seperti sambungan internet pribadi yang aman, bukan jaringan WiFi publik.
- Perlu mempertimbangkan pengaturan perangkat komputer kantor secara terpusat, yaitu hanya admin IT yang bisa memasang aplikasi.
- Pastikan awak media pemegang perangkat komputer/laptop menjalankan prinsip-prinsip keamanan digital. Detail panduan keamanan perangkat ada pada Bab 2 **Panduan Keamanan Digital Jurnalis**[6].

3. Router

   Router adalah alat yang berfungsi menghubungkan perangkat ke internet atau jaringan lain serta mengelola lalu lintas data. Tempatkan *router* pada lokasi yang aman dari ancaman fisik seperti pencurian atau perusakan. Sembunyikan *router* jika tidak ingin jaringan WiFi diketahui publik.

4. Kamera pengawas
   - Pasang kamera pengawas (CCTV) di titik-titik yang bisa mengaver sudut-sudut objek vital (seperti ruang penyimpanan dokumen dan perangkat), akses masuk, dan ruang publik di kantor.
   - Kamera pengawas hanya terhubung dengan jaringan internal yang tidak bisa diakses oleh pihak luar.

[6] https://aji.or.id/system/files/2024-07/layoutpanduankeamanandigitaluntukjurnalisfixcompressed_4.pdf

C. Keamanan Web[7]

Bagi sebuah perusahaan media, situs web merupakan salah satu aset digital terpenting karena menjadi rumah penyebaran konten. Situs web juga menjadi medium utama perusahaan media untuk mendapatkan pemasukan finansial. Karenanya, perlindungan situs web adalah hal vital bagi perusahaan media.

Situs web juga berpotensi menjadi target serangan digital terhadap media seperti *Distributed Denial of Service* (DDoS), *deface*, hingga pengambilalihan akun pengelola. Berdasarkan riset AJI Indonesia dan PR2 Media pada 2024, DDOS menjadi jenis serangan terbanyak kedua yang dialami oleh perusahaan media di Indonesia.

Sejalan dengan temuan survei itu, berdasarkan data laporan kasus yang dihimpun laman advokasi.aji.or.id, dari 16 kasus serangan terhadap jurnalis dan media selama 2023, tiga di antaranya adalah kasus DDOS, tiga kasus *defacement* situs web, dan satu kasus suspend situs web.

Ada sejumlah faktor yang membuat situs web sebuah lembaga, termasuk situs media berisiko mengalami serangan. Faktor-faktor tersebut antara lain informasi dan yang disebarkan oleh sebuah media, siapa yang berpeluang melakukan serangan atau gangguan (orang, kelompok, atau lembaga yang menjadi musuh/memiliki kepentingan berlawanan), dan sumber daya yang dimiliki perusahaan media untuk memproteksi situs web tersebut.

a. Mengidentifikasi Ancaman

Salah satu ancaman terbesar yang kerap terjadi terhadap situs web media adalah DDOS. Situs web yang terkena DDOS menjadi sulit diakses oleh publik atau dalam bentuk paling ringan adalah lambatnya akses. Bagi media yang telah menerapkan proteksi seperti penggunaan sistem anti-

[7] Langkah-langkah tentang keamanan web juga dapat dibaca melalui link berikut: https://github.com/OpenInternet/MyWebsiteIsDown/blob/master/MyWebsiteIsDown.md

DDOS memadai, dampak serangan bisa jadi tidak terlalu besar. Namun, bagi situs media yang tidak memiliki perlindungan, dampak DDOS bisa berlangsung lama dan tak kunjung pulih.

Sebagai langkah mitigasi awal, evaluasi risiko akan membantu menentukan langkah pencegahan yang diperlukan.

1) Apa yang harus dilindungi?
   Identifikasi tiga hal ini:
   - Tipe data atau informasi yang ada dalam situs web tersebut.
   - Tipe data atau informasi yang ditampilkan situs web tersebut.
   - Kepada siapa informasi dalam situs tersebut disajikan (audiens)?

   Identifikasi ini sangat penting dalam mitigasi masalah pada situs web yang mungkin terjadi, misalnya potensi terkena serangan DDOS. Saat mengalami serangan DDOS, pengelola situs web maupun pengunjung (*visitor*) kehilangan akses sementara terhadap konten-konten dalam situs. Pengelola web juga tidak bisa memublikasikan informasi melalui situs web itu hingga pulih.

   Berdasarkan identifikasi tiga hal tersebut, pengelola media/situs web bisa mengevaluasi apa yang dibutuhkan untuk memproteksinya. Selain itu, apa yang bisa dilakukan untuk mencegah dampak yang mungkin terjadi saat publik tidak bisa mengakses konten dalam situs tersebut akibat DDOS atau serangan lain.

2) Pihak yang berpotensi mengganggu situs web
   Sulit mengenali siapa yang berpotensi ingin menyerang situs web. Aktor serangan bisa jadi orang yang berkepentingan dengan informasi yang dibagikan melalui situs tersebut dan bisa jadi berganti-ganti setiap waktu.

   Serangan DDOS dan *deface* bisa jadi muncul mengiringi kasus-kasus yang sensitif atau event tertentu seperti pemilu atau pengungkapan

sebuah kasus. Pertanyaan-pertanyaan berikut bisa membantu mengidentifikasi para aktor yang berpotensi melakukan serangan.

- Apa yang dipublikasikan situs media Anda?
- Siapa atau apa yang sering dikritik melalui pemberitaan di situs media Anda?
- Siapa yang memiliki kepentingan atau terdampak kritik dari informasi di situs media Anda?
- Siapa pesaing media Anda?
- Siapa saja pengunjung situs media Anda?
- Seberapa besar dampak situs media Anda?

Jika Anda menemukan pihak yang berpotensi menjadi musuh, pertanyaan berikutnya adalah apa motivasi mereka jika hendak menyerang situs media Anda. Selain itu, apa manfaat serangan itu bagi mereka.

3) Investasi

Ada sejumlah pertanyaan yang perlu diajukan untuk mengukur seberapa siap menghadapi serangan terhadap situs web.

- Seberapa besar dana yang dimiliki perusahaan media Anda untuk membangun sistem keamanan web?
- Perlindungan apa saja yang perusahaan media Anda terapkan untuk merespons serangan yang mungkin terjadi, misalnya DDOS?
- Seberapa kuat kompetensi teknis sumber daya manusia di perusahaan media yang khusus menangani keamanan web?

Tidak ada standar anggaran minimal atau solusi tunggal untuk membangun proteksi web bagi lembaga atau perusahaan media. Bagi media besar, investasi keamanan web bisa jadi sangat besar. Sebaliknya bagi media dengan sumber daya kecil, upaya membangun proteksi membutuhkan pendekatan berbeda.

- Bagi pengelola situs web sebuah perusahaan media kecil, *hosting* situs web pada platform yang menyediakan perlindungan terhadap DDOS bisa menjadi pilihan. Pilihan ini tidak membutuhkan banyak sumber daya manusia khusus untuk keamanan web.

- Bagi perusahaan media besar, merekrut ahli untuk membangun sendiri situs web dan membangun sistem proteksi sendiri bisa menjadi pilihan.

b. Mengidentifikasi Serangan (Jika Situs Bermasalah/Down)

Ketika situs mengalami masalah atau *down*, ada beberapa kemungkinan masalah. Misalnya ada eror dalam pemrograman, masalah teknis pada penyedia layanan *hosting* web, atau masalah administrasi. Karenanya, penting mengidentifikasi penyebab masalah pada situs web.

1) Muncul pesan "*error*"

- Ketika muncul pesan adanya "*error*", bisa jadi ada masalah pada *software*. Pengelola situs perlu mengidentifikasi perubahan apa yang telah dibuat dan mungkin menyebabkan eror.
- Jika tidak bisa diatasi, pengelola situs bisa menghubungi *webmaster* untuk memberitahukan masalah tersebut, lengkap dengan tangkapan layar pesan "*error*" itu atau kronologinya.

2) Muncul pesan dari penyedia web *hosting*

- Hal ini bisa jadi menunjukkan ada persoalan hukum atau administrasi seperti masalah hak cipta (*copyright*), tagihan atau *billing* biaya *hosting* atau berlangganan layanan dari platform tertentu, atau masalah lain.
- Jika ada dugaan masalah terkait hak cipta, cek penggunaan material seperti teks, gambar, video, suara atau lagu, dan lainnya yang diambil dari pihak lain.

3) Situs tidak bisa loading sama sekali

- Hal ini bisa disebabkan adanya masalah pada penyedia *hosting* web.
- Cek situs perusahaan *provider hosting* web. Jika situs tersebut bermasalah atau tidak bisa diakses, bisa jadi *provider* tersebut sedang bermasalah atau sedang dalam pemeliharaan (*maintenance*) yang terjadwal.
- Cek akun media sosial provider tersebut seperti di X atau lainnya,

atau cari informasi tentang *provider* tersebut untuk melihat apakah ada masalah serupa yang sedang diperbincangkan oleh warganet.

4) Situs tidak tersedia meskipun web *hosting* normal

- Cek http://www.isup.me/ untuk mengidentifikasi apakah yang bermasalah situs tersebut atau jaringan Anda yang bermasalah.
- Jika muncul keterangan "It's just you. <nama situs> is up." berarti jaringan atau internet Anda yang bermasalah.

5) Kemungkinan terkena sensor

- Jika situs Anda tidak bisa diakses, cobalah mengakses situs-situs lain yang terkait atau memiliki konten yang menyajikan isu-isu serupa. Jika situs-situs tersebut tidak bisa diakses, bisa jadi ada penyensoran.
- Coba mengakses situs tersebut melalui peramban Tor atau Psiphon atau menggunakan VPN. Jika bisa diakses melalui cara tersebut, ada kemungkinan situs Anda terkena sensor di dalam negeri.

6) Loading situs melambat/tidak stabil

- Jika *loading* situs tidak stabil, terkadang bisa diakses dan terkadang terputus, atau lambat tidak seperti biasa, bisa jadi jumlah kunjungan atau permintaan akses terhadap laman situs tersebut.
- Cek *traffic* kunjungan situs, misalnya melalui Google Analytic. Jika terdapat peningkatan pengunjung dan masih terbilang normal, berarti ada masalah performa pada situs Anda.
- Hubungi *webmaster* atau *provider hosting* web untuk meningkatkan performa situs, misalnya dengan penambahan *plugin* tertentu.
- Pertimbangkan menggunakan *plugin* yang membantu melakukan *cache* (menyimpan data di jaringan server). *Cache* bisa mempercepat akses terhadap situs dan meningkatkan performa saat *traffic* kunjungan sedang tinggi.

7) Kemungkinan DOS/DDOS

- Jika diagnosis di atas tidak menemukan masalah yang tepat,

misalnya situs tetap sulit diakses dan performa tetap buruk, bisa jadi situs sedang mengalami serangan *Denial Of Service* (DOS).

- DOS bisa dilakukan seorang penyerang yang ingin mengakses sebuah situs web berkali-kali menggunakan *tool* otomatis untuk menyulitkan pembaca lain mengakses situs itu. Jika dilakukan satu orang, serangan itu tidak menyebabkan masalah serius.
- Namun, DOS umumnya dilakukan oleh seorang penyerang menggunakan ribuan mesin (*distributed* DOS atau DDOS) yang bertujuan melumpuhkan situs tersebut sehingga tidak bisa lagi diakses oleh pembaca yang sebenarnya.

c. Mitigasi Serangan DDOS

Ada sejumlah layanan yang menyediakan perlindungan dari sebelum terjadi serangan hingga pemulihan selama dan setelah terjadi serangan. Saat terjadi serangan, layanan tersebut membutuhkan waktu sedikitnya tiga hari untuk memunculkan alamat baru yang terlindungi. Karenanya, mitigasi sejak dini lebih efektif daripada menunggu serangan datang.

Ada banyak layanan yang bisa membantu sebuah situs merespons serangan DOS/DDOS. Secara umum terdiri atas 2 kategori, yaitu *hosted service* dan *proxied services*.

1) Hosted services

Hosted services mengharuskan pengelola memindahkan situs web ke *server provider*. *Provider hosting* biasanya menawarkan perlindungan yang terintegrasi, baik perlindungan terhadap serangan DDOS maupun jenis serangan lain. Namun, layanan seperti ini lebih mahal (bisa hampir US$500 atau Rp8 juta per bulan). Selain itu, provider memiliki kendali penuh atas situs web kita.

a) Kelebihan:

- Menyediakan layanan perlindungan yang terpusat.
- Ada layanan lain seperti konsultasi.
- Dukungan penuh dari penyedia layanan.

b) Kekurangan:

- Kendali situs web diserahkan kepada penyedia layanan.
- Pemilik situs web harus berhati-hati memilih layanan yang tepercaya.
- Lebih mahal.

c) Contoh layanan:

VirtualRoad.org

- Biaya mulai €100 (Rp1,7 jutaan) per bulan. *Hosting* yang lebih kompleks membutuhkan biaya yang lebih besar.
- VirtualRoad.org merupakan bagian dari proyek Media Frontiers, lembaga sosial dari Denmark yang didirikan oleh International Media Support (IMS).
- Layanan tambahan: transfer situs web ke sistem *provider*, pendaftaran *domain*, *optimization*, audit keamanan, perlindungan terhadap *hacking* dan *phishing*, pemberian laporan keamanan terkait upaya-upaya serangan, dan dukungan aspek hukum.
- Tautan ke layanan: https://virtualroad.org/get-protected/packages dan https://virtualroad.org/contact atau *e-mail* info@virtualroad.org.

The Positive Internet Company

- Biaya mulai $495 (Rp7,8 juta) per bulan dengan *server* yang dikelola sepenuhnya (*full served server*) untuk sebuah situs web. Pilihan lain dengan *shared hosting* seharga £125 (Rp2,6 juta) per tahun.
- The Positive Internet Company merupakan perusahaan nonprofit yang berpusat di Inggris dan Amerika Serikat.
- Layanan tambahan: *firewalls*, pengelolaan *database*, dan *backup*.
- Tautan ke layanan: http://www.positive-internet.com/services/vip-hosting dan http://www.positive-internet.com/contact-us atau e-mail good@positive-internet.com.

2) Proxied services

Proxied services (layanan proksi) bisa menjadi pilihan jika pengelola ingin tetap memiliki kendali dan meng-hosting sendiri situs web sehingga pengaturan lebih mudah. Penyedia layanan memiliki banyak server di

berbagai tempat di dunia yang akan melindungi situs web dari traffic yang tidak wajar. Pelindungan ini dilakukan dengan mirroring dan menyajikan salinan situs web kita yang selalu diperbarui.

a) Kelebihan:

- Biaya lebih murah (ada yang dimulai dari level gratis).
- Pengaturan lebih cepat dan mudah
- Tidak perlu mengganti *hosting* situs web.
- Punya opsi tidak melepas layanan kapan saja.

b) Kekurangan:

- Tidak banyak dukungan selain perlindungan terhadap serangan DDOS.
- Tidak banyak layanan tambahan berupa anti-malware atau anti-spam.
- Lalu lintas data terenkripsi melalui *Secure Socket Layer* (SSL) atau dikenal HTTPS, bisa cepat terdekripsi dan kembali terenkripsi lagi oleh server proksi. Jika lalu lintas data terdekripsi, maka terbuka celah bagi penyerang.

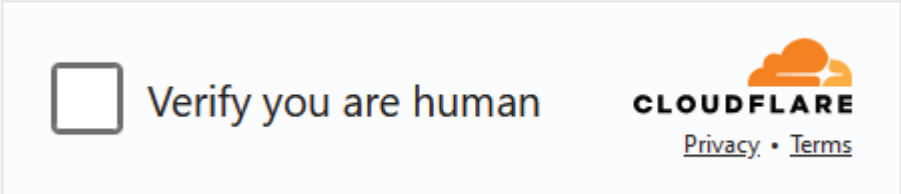
c) Contoh layanan:

Deflect

- Biaya gratis.
- Ditujukan bagi situs web milik NGO, pembela HAM, dan media independen.
- Deflect merupakan proyek *open source* eQualit.ie, sebuah kolektif teknologi nonprofit di Montreal, Kanada. Deflect didanai NGO dan pemerintah beberapa negara termasuk Amerika Serikat untuk melindungi kebebasan berpendapat. Deflect tidak mengungkap ke publik situs web mana saja yang dilindungi dan tidak membutuhkan persetujuan untuk memberikan layanan.
- Layanan tambahan: tim Deflect memiliki beberapa *grant* untuk mendanai sertifikat SSL tambahan dan biaya proteksi lainnya.
- Tautan layanan: https://wiki.deflect.ca/signup/ atau https://wiki.deflect.ca/wiki/Join_Deflect.

CloudFlare

- Biaya: gratis untuk level *basic*, $20 per bulan dengan tambahan dukungan SSL, dan $200 per bulan untuk kebutuhan lebih besar.
- Ada pembatasan subjek penerima layanan berdasarkan kebijakan luar negeri Amerika Serikat (lihat https://blog.cloudflare.com/thoughts-on-abuse).
- Cloudflare merupakan layanan dari perusahaan yang berbasis di San Francisco untuk perusahaan profit. Cloudflare melindungi *server* di berbagai belahan dunia dan tunduk pada aturan hukum beberapa negara.
- Cloudflare banyak dipakai oleh beragam situs, dari milik media besar seperti The New York Times dan BBC, hingga sejumlah situs media nasional di Indonesia.
- Tautan layanan: https://www.cloudflare.com/sign-up.



Google's Project Shield/PageSpeed

- Biaya: PageSpeed gratis untuk masa *trial*; Project Shield ditawarkan secara gratis bagi pihak *tester* yang dipercaya.
- Pengguna layanan harus mendapatkan persetujuan (dalam 2 jam). Beberapa organisasi atau negara bisa mengalami pembatasan. Sedangkan Project Shield hanya bisa digunakan oleh organisasi yang diundang dan hanya menerima permintaan dari situs web yang berisi konten berita, HAM, atau pemilu.
- Layanan disediakan oleh Google. Inc. yang tunduk pada hukum di negara-negara tertentu termasuk Amerika Serikat.
- Tautan Pagespeed: https://developers.google.com/speed/pagespeed/service. Tautan Project Shield: http://projectshield.withgoogle.com/about/.

d. Backup Data

Backup data secara reguler sangat penting dalam mitigasi serangan DDOS. Saat situs lumpuh karena DDOS, pengelola bisa mengembalikan data dengan cara mengimpor data *backup* yang disimpan di sistem lain yang terpisah.

1) Hosted Service

Ada dua cara mem-backup data situs web yang menggunakan *hosted service*, yaitu ekspor data dari seluruh laman, postingan, serta komentar ke dalam sebuah *file* XML dan *mirroring website* (salinan situs web utama yang di-*hosting* di server lain).

File XML hanya memuat data dalam bentuk teks dan tidak bisa membuat kopian file berbentuk gambar dan lainnya. Untuk memastikan situs kita memiliki *backup* adalah membuat *mirroring website*, yaitu salinan situs web pada *server* lain.

2) Shared Hosting

Pengelola bisa menyalin seluruh file dari situs web dan menyimpan cuplikan (*snapshot*) *database* situs tersebut.

3) Web Server Milik Sendiri

Pengelola situs web dengan *server* sendiri harus bisa melakukan sendiri *backup* otomatis ke sebuah *server* terpisah.

D. Keamanan Komunikasi

1. Menggunakan aplikasi percakapan terenkripsi
   a. Gunakan aplikasi percakapan yang memberikan fungsi enkripsi ujung ke ujung (*end to end encryption*). Enkripsi dari ujung ke ujung artinya sistem komunikasi yang hanya bisa dibaca oleh pengguna yang berkomunikasi.
   b. Hindari menggunakan WhatsApp untuk berkomunikasi terkait informasi yang berisiko tinggi. Meskipun diklaim sudah menggunakan enkripsi

ujung ke ujung, Whatsapp rentan diserang karena popularitasnya berdasarkan sejumlah kasus peretasan.

c. Gunakan alternatif aplikasi percakapan yang menyediakan fasilitas untuk menghancurkan pesan secara otomatis, seperti Telegram, Signal, dan Wire.
d. Matikan fungsi pencadangan otomatis terutama jika aplikasi itu untuk percakapan berisiko tinggi.
e. Kombinasikan penggunaan aplikasi percakapan berbeda-beda agar bisa memecah komunikasi.

2. Memantau keamanan percakapan

a. Jika tim redaksi masih menggunakan Whatsapp, pastikan notifikasi keamanan diaktifkan.
b. Pada Whatsapp, aktifkan "s*ecurity notification*". Buka *Settings*, pilih *Account,* pilih *Security*, pastikan status "*Show security notifications on this device*" tercentang.
c. *Chat* yang terenkripsi secara *end-to-end* antara Anda dan pengguna lain memiliki kode keamanan tersendiri yang digunakan untuk memverifikasi bahwa panggilan dan pesan yang Anda kirim ke *chat* tersebut terenkripsi secara *end-to-end*.
d. Kode keamanan dapat ditemukan di layar info kontak sebagai kode QR dan juga angka 60 digit. Kode ini bersifat unik untuk setiap *chat* individual dan dapat dibandingkan dengan orang yang berada di setiap *chat* untuk memverifikasi bahwa pesan yang dikirim terenkripsi secara *end-to-end*.
e. Jika *security notification* diaktifkan, kita bisa melihat notifikasi seandainya ada perubahan kode keamanan pada akun Whatsapp dalam daftar kontak kita.
f. Perhatikan jika ada notifikasi perubahan kode keamanan pada kontak kita. Notifikasi ini muncul jika:
   - kontak kita baru saja menginstal ulang WhatsApp,
   - mengganti perangkat telepon,
   - atau menambah/menghapus perangkat yang ditautkan.
g. Notifikasi ini sekaligus bisa menjadi pengingat "jangan-jangan akun WhatsApp teman dalam daftar kontak kita diambil alih orang lain".

h. Pada Signal, ada nomor keamanan (*safety number*). Setiap obrolan pribadi Signal memiliki nomor keamanan unik yang memungkinkan pengguna memverifikasi keamanan pesan dan panggilan Anda dengan kontak tertentu.
i. iSerupa pada Whatsapp, kode ini dapat ditemukan pada layar info kontak sebagai kode QR dan juga angka 60 digit. Untuk melihatnya:
   - Buka percakapan dengan kontak Anda
   - Ketuk tanda titik tiga, pilih *Conversation settings*.
   - Pilih *view safety number* (lihat nomor keamanan).
j. Signal akan memberitahu kita jika ada nomor keamanan atau *safety number* kontak kita yang berubah. Hal ini memungkinkan pengguna memeriksa privasi percakapan dengan kontaknya dan mengantisipasi adanya serangan.
k. Ketika sebuah kontak beralih ke ponsel baru atau menginstal ulang Signal, kita akan menerima peringatan perubahan nomor keamanan.
l. Jika nomor keamanan berubah berkali-kali atau mendadak, bisa jadi ada yang salah dan kita perlu mengecek pemilik nomor.

3. Memilih dan mengelola peramban (*browser*)
   a. Gunakan peramban yang memberikan pilihan privasi pada penggunanya, seperti Firefox dan Brave. Sejumlah peramban menyimpan aktivitas kita, mulai website yang pernah dibuka, kata kunci, IP *address*, lokasi dll.
   b. Aturlah agar hanya seminimal mungkin aktivitas pribadi yang direkam oleh peramban tersebut. Perbandingan privasi dan keamanan peramban bisa dicek di https://www.mozilla.org/en-US/firefox/browsers/compare/.
   c. Pengaturan privasi dan keamanan pada Chrome bisa dicek di chrome://settings/privacy. Sedangkan pengaturan privasi dan keamanan pada Firefox bisa dicek di about:preferences#privacy. Periksa jejak digital yang direkam oleh peramban tersebut dan pikirkan ulang apakah Anda memang harus membiarkannya direkam atau tidak.
   d. Bersihkan riwayat penelusuran atau aktivitas daring yang tersimpan di peramban.

e. Jangan pernah merekam identitas ataupun aset digital yang berisiko tinggi, seperti kata sandi, nomor kartu kredit, dan semacamnya.
f. Pilihlah agar semua akun Anda akan otomatis keluar ketika peramban ditutup

4. Memastikan keamanan protokol situs/laman
   a. Pastikan situs web yang kita akses sudah menggunakan protokol https (*hypertext transfer protocol secure*) bukan http.
   b. Jangan memasukkan nama pengguna dan kata sandi pada situs web yang masih menggunakan protokol http, misalnya untuk membuka *email* atau akun media sosial, dan rekening bank.

5. Menambah *plugin* atau *add-ons* tertentu untuk deteksi awal

   Ada beberapa *plugin* atau *add-ons* yang dapat berfungsi untuk meningkatkan keamanan dan memberikan pemberitahuan (*alert*) saat terjadi aktivitas yang mencurigakan saat Anda berkomunikasi menggunakan internet.

   a. Privacy Badger berguna untuk mengetahui aplikasi apa saja yang merekam aktivitas Anda saat mengunjungi situs tertentu. Tambahkan *add-ons* Privacy Badger untuk Mozilla di tautan https://addons.mozilla.org/en-US/firefox/addon/privacy-badger17/. Sedangkan untuk Chrome, tambahkan dari tautan https://chrome.google.com/webstore/detail/privacy-badger/pkehgijcmpdhfbdbbnkijodmdjhbjlgp.
   b. HTTPS Everywhere berguna untuk mengenkripsi protokol situs web yang belum menggunakan https. Untuk Mozilla tambahkan dari tautan https://addons.mozilla.org/en-US/firefox/addon/https-everywhere/ dan Chrome dari https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclmclpchllfjekcdonpmejbdp?hl=en. Opsi lainnya, pengguna Mozilla bisa mengatur peramban hanya mengakses situs https dengan mengaktifkan HTTPS-Only Mode pada about:preferences#privacy tanpa perlu memasang plugin.
   c. Cookie AutoDelete berguna untuk menghapus cookies (remah-remah jejak digital) begitu kita menutup peramban. Bagi pengguna Chrome, tambahkan melalui tautan https://chrome.google.com/webstore/detail/cookie-autodelete/fhcgjolkccmbidfldomjliifgaodjagh?hl=en.

Bagi pengguna Mozilla, tambahkan melalui: https://addons.mozilla.org/en-US/firefox/addon/cookie-autodelete/.

6. Berbagi berkas pekerjaan (*file sharing*)
   Gunakan layanan berbagi berkas yang lebih peduli pada keamanan daripada Google workspace. Alternatif yang tersedia yakni:
   a. Untuk berbagi dokumen pekerjaan secara bersama-sama, gunakan www.cryptpad.fr.
   b. Untuk berbagi berkas dalam ukuran besar bisa menggunakan https://send.tresorit.com/.
   c. Untuk berbagi dokumen ataupun berkas lain dengan www.mega.nz.

7. Menyamarkan jejak komunikasi dengan VPN
   a. Gunakan *virtual private network* (VPN) jika mengakses wifi di tempat umum seperti kafe, hotel, bandara, dan lain-lain. Begitu pula saat terpaksa membuka situs http.
   b. WiFi publik, seperti yang ada di kafe, bandara, atau hotel, sering kali tidak memiliki enkripsi yang cukup kuat, membuatnya rentan terhadap serangan *Man-in-the-Middle* dan pencurian data. Tanpa VPN, data pribadi seperti kata sandi, informasi kartu kredit, atau riwayat *browsing* bisa dengan mudah disadap oleh pihak ketiga yang berbahaya. VPN mengenkripsi koneksi internet kita, sehingga menjaga data kita tetap aman meskipun sedang menggunakan jaringan WiFi publik yang tidak terlindungi.
   c. Jangan menggunakan sembarang layanan VPN dan tidak asal gratis karena berpotensi membahayakan keamanan seperti mengambil data pribadi, meminta akses terhadap informasi sensitif, hingga meminta akses memindai aplikasi yang terinstal di perangkat kita. Beberapa layanan VPN yang lebih aman antara lain Proton VPN dan Mullvad.
   d. Jika tidak mampu menggunakan VPN berbayar, gunakan VPN yang menawarkan pelindungan tanpa terlalu banyak pembatasan pada versi gratis seperti Proton VPN. Proton VPN masih direkomendasikan karena dikembangkan developer dari Swiss dan berada di bawah hukum Swiss, negara yang mengedepankan perlindungan data pribadi.

Jika memilih versi yang tidak berbayar, pilihan server (peladen) sangat sedikit tetapi bisa diakses tanpa batasan waktu maupun kuota.

8. Memilih surel (*email*) yang aman
   a. Gunakan layanan *email* yang menyediakan fungsi enkripsi seperti Rise Up, Protonmail, Disroot, dan Tutanota.
   b. Tambahkan fungsi enkripsi pada email kantor seperti PGP-Key atau Enigmail pada aplikasi pengelola surel Thunderbird.
   c. Tambahkan aplikasi enkripsi seperti Mailvelope pada layanan *email* yang tidak terenkripsi.

9. Memeriksa lampiran dan tautan
   a. Jika Anda menerima email berisi tautan (*link*) dan lampiran (*attachment*) dari orang yang tidak dikenal sama sekali, hindari langsung membuka tautan dan lampiran tersebut. Bisa saja, tautan atau lampiran tersebut telah ditanam *malware* yang bisa menginjeksi laptop/*handphone* Anda. *Malware* dapat mematai-matai aktivitas (*spyware*) atau mencuri data dari perangkat.
   b. Periksalah tautan dan lampiran tersebut secara daring pada platform pemeriksa keamanan seperti https://urlscan.io/ atau https://www.virustotal.com/gui/home/upload.

10. Menggunakan mesin pencari yang aman
    a. Gunakan mesin pencari yang tidak merekam jejak pencarian, seperti DuckDuckGo
    b. (https://duckduckgo.com/), StartPage (https://www.startpage.com/), atau Qwant
    c. (https://www.qwant.com/).

11. Detail panduan keamanan komunikasi ada pada Bab 4 **Panduan Keamanan Digital Jurnalis**[8].

[8] https://aji.or.id/system/files/2024-07/layoutpanduankeamanandigitaluntukjurnalisfixcompressed_4.pdf

BAB VII
Mekanisme Penanganan

Ada beberapa langkah yang perlu dilakukan saat perusahaan media atau awak media menjadi sasaran serangan digital atau menyadari sedang menjadi target serangan.

1. **Jangan panik, tenangkan pikiran sebelum merespons serangan.**
   Reaksi panik dapat memperburuk situasi dan mengarah pada keputusan yang terburu-buru, seperti memberikan informasi sensitif, mengklik tautan berbahaya, atau melakukan tindakan yang memperbesar kerugian. Dengan menjaga ketenangan, kita bisa lebih objektif dalam menilai ancaman, mengambil langkah yang lebih terencana untuk mengatasi serangan, seperti memutuskan koneksi internet, mengganti kata sandi, atau melaporkan insiden kepada pihak berwenang atau profesional. Mengendalikan emosi juga memungkinkan kita untuk bertindak dengan lebih efisien dalam mencegah atau memitigasi dampak dari serangan digital tersebut.

2. **Lakukan langkah-langkah darurat untuk mengidentifikasi masalah**
   Langkah-langkah darurat untuk mengidentifikasi masalah serangan digital adalah sebagai berikut:
   1. Putuskan koneksi internet: segera cabut atau nonaktifkan koneksi internet untuk mencegah penyebaran atau dampak lebih lanjut dari serangan.

2. Periksa aktivitas yang mencurigakan: tinjau aktivitas perangkat dan akun yang terlihat tidak biasa, seperti *login* yang tidak dikenali, perubahan pengaturan, atau *file* yang hilang atau muncul tiba-tiba.
3. Jalankan pemindai keamanan (antivirus): gunakan perangkat lunak antivirus atau pemindai keamanan yang diperbarui untuk mendeteksi *malware* atau virus yang ada pada perangkat.
4. Ubah kata sandi: ganti kata sandi pada akun yang terhubung dengan perangkat yang diserang dan pastikan untuk mengaktifkan verifikasi dua langkah (2FA).
5. Periksa riwayat log dan aktivitas: untuk akun atau aplikasi *online*, jika masih bisa diakses, cek riwayat *login* dan aktivitas untuk melihat jika ada akses yang tidak sah.
6. Cadangkan data penting: segera cadangkan data penting yang masih aman untuk mencegah kehilangan informasi yang lebih besar.
7. Hubungi penyedia layanan atau profesional keamanan: jika perlu, hubungi pihak yang memiliki kapasitas/profesional dalam keamanan siber atau organisasi masyarakat sipil yang bisa menangani serangan siber (misalnya Tim Reaksi Cepat atau TRACE) untuk mendapatkan bantuan lebih lanjut dan memperbaiki kerusakan.
8. Laporkan serangan: laporkan serangan ke layanan penyedia aplikasi atau platform *online* untuk pemulihan akun atau polisi jika diperlukan.

3. Dokumentasikan kondisi yang terjadi pada akun Anda

- Segera dokumentasikan isi pesan (*e-mail* atau *direct messenger*), notifikasi, atau tanda-tanda lain yang muncul.
- Cara dokumentasi yang paling mudah adalah merekam tangkapan layar (*screenshot*) lalu simpan rekaman itu sebagai bukti.

4. Susun kronologi terjadinya serangan

Dalam kondisi panik, hal ini tidak begitu mudah. Maka itu tenangkan pikiran dengan cara bertanya pada diri sendiri, kapan pertanda awal kondisi digital yang tidak wajar, hilangnya akses, hingga upaya terakhir yang dilakukan untuk merespons serangan. Ambil alat pencatat, segera catat apa yang diingat berdasarkan kronologi waktu.

Berikut langkah darurat yang bisa dilakukan di awal untuk merespons serangan:

A. Serangan terhadap situs web

Untuk merespons serangan terhadap situs web, kembalilah ke angka VI (Mekanisme Pencegahan dan Mekanisme Penanganan), bagian C (Keamanan Web) huruf b (Mengidentifikasi Serangan) dan huruf c (Mitigasi Serangan DDOS) pada panduan ini.

B. Hilangnya Akses Terhadap Akun

Akun *email*, media sosial, dan platform percakapan menjadi medium vital bagi perusahaan media untuk menyebarluaskan produk jurnalistik, termasuk yang menyangkut isu-isu sensitif. Karenanya, akun sangat mungkin menjadi target serangan.

Salah satu dampak serangan adalah hilangnya akses terhadap sebuah akun platform digital. Jika itu terjadi, pastikan Anda melakukan langkah berikut:

1. Identifikasi masalah

a. Pastikan *username* dan *password* yang Anda masukkan benar, tidak ada kesalahan tulis (*typo*) termasuk posisi *capslock*.
b. Ingat kapan kali terakhir mengganti password dan masukkan password terakhir yang dibuat.
c. Cek akses terakhir yang dilakukan admin (jika admin lebih dari 1 orang). Pastikan tidak ada admin yang menghapus akun. Jika akun dihapus (oleh admin maupun orang lain), maka akun tidak bisa dikembalikan.
d. Cek apakah Anda masih bisa mengakses akun *email* terkait akun (*email* pemulihan) dan nomor ponsel terkait.
e. Cek inbox *email* terkait akun, apakah ada notifikasi yang menunjukkan ada upaya masuk (*login*) dari perangkat yang tidak Anda kenal.
f. Jika yang bermasalah adalah akun media sosial, lihat profil akun Anda (lewat akun lain atau mesin pencari), apakah ada yang berubah atau ada postingan yang tidak pernah Anda unggah.
g. Jika ada yang postingan yang hilang, muncul postingan yang diunggah bukan oleh Anda, ada notifikasi akses dari perangkat asing, atau ada indikasi perubahan *email*/nomor pemulihan yang tidak Anda lakukan, berarti akun Anda diambil alih orang lain.

h. Jika *username* dan *password* sudah dipastikan benar, hal yang mungkin terjadi adalah akun Anda diblok atau di-*suspend* oleh platform. Hal ini bisa terjadi karena akun Anda dilaporkan secara masif oleh akun-akun lain atau karena dianggap melanggar panduan komunitas (*community guidelines*).

2. Peretasan Whatsapp

a. Pastikan apakah akun Whatsapp benar-benar diretas. Jika akun Whatsapp Anda tiba-tiba keluar (*logout*) dari perangkat, itu adalah indikasi bahwa ada orang lain yang berusaha mengakses akun tersebut dari perangkat lain.
b. Jika akun Whatsapp hanya keluar dari perangkat dan belum mengirim pesan ke nomor lain, kemungkinan besar pelaku belum berhasil menguasai nomor Anda karena harus memasukkan PIN (jika Anda mengaktifkan *Two-Step Verification* pada akun Whatsapp.
c. Jika akun Whatsapp itu sudah mengirim pesan ke nomor lain, artinya pelaku sudah berhasil menguasai akun Anda dan menggunakannya dari perangkat lain. Situasi ini lebih susah ditangani, apalagi jika pelaku sudah mengaktifkan 2FA.
d. Lakukan prosedur berikut:
    - Copot/*uninstall* Whatsapp dari ponsel Anda dan install kembali.
    - Daftarkan nomor Anda dan tunggu kode verifikasi melalui SMS dan masukkan segera kode verifikasi 6 digit yang dikirim via SMS.
    - Jika Anda tidak menerima kode 6 digit melalui SMS, tunggu hingga proses selesai dan coba lagi. Waktu tunggu dapat berlangsung hingga 10 menit.
    - Jika waktu berakhir sebelum Anda menerima kode verifikasi, akan ada opsi meminta panggilan telepon. Pilih opsi “Panggil saya” untuk meminta panggilan telepon.
    - Ketika Anda menerima panggilan, mesin suara otomatis akan memberitahukan kode verifikasi 6 digit. Masukkan kode ini untuk memverifikasi akun Whatsapp Anda.
    - Saat akun Anda kembali, segera tambahkan PIN dan *email* agar akun Whatsapp Anda tidak dicuri kembali.
    - Apabila Anda masih sulit masuk dan diminta untuk

memasukkan kode verifikasi dua langkah, peretas mungkin telah mengaktifkan PIN di Whatsapp tersebut. Anda harus menunggu 7 hari sebelum dapat masuk ke akun tanpa kode verifikasi dua langkah.

- Laporkan bahwa akun Anda telah dicuri ke alamat email: support@whatsapp.com dengan subyek "Hilang/Dicuri: Silakan nonaktifkan akun saya" di badan email.

3. Peretasan akun Gmail

a. Jika Anda masih bisa mengakses akun Gmail Anda, segera ubah *password* dan tambahkan autentikasi 2 langkah (bagi yang belum mengaktifkannya).
b. Apabila Anda tidak bisa *login*, buka halaman pemulihan akun dengan klik tautan https://s.id/PemulihanGmail. Anda akan diminta memasukkan akun *recovery* (pemulihan) dan ikuti petunjuk berikutnya untuk mendapatkan kembali akses *login* ke akun *email* Anda.
c. Selengkapnya mengenai peretasan dan pemulihan akun Gmail, bisa mengikuti langkah-langkah dalam tautan ini https://support.google.com/accounts/answer/7682439?hl=id.

4. Peretasan Yahoo Mail

a. Reset *password* Anda dengan masuk ke tautan https://help.yahoo.com/kb/SLN27051.html.
b. Masukkan alamat *email* akun Yahoo Mail Anda.
c. Pilih metode reset yang diinginkan, melalui nomor HP atau *email* pemulihan yang sudah Anda daftarkan. Pemulihan melalui *email* lebih direkomendasikan daripada nomor HP.
d. Selanjutnya, sebuah kode akan dikirimkan ke *email* pemulihan atau via SMS. Masukkan kode itu ke halaman Yahoo.
e. Buat *password* baru yang lebih kuat dengan kombinasi angka, huruf dan spasi.

5. Pengambilalihan Akun Facebook

a. Untuk mengetahui apakah ada orang lain yang mengakses akun Anda secara diam-diam, cek Pengaturan (*setting*) - Keamanan dan Info *Login*. Lalu periksa "Tempat Anda *Login*" untuk mengecek daftar perangkat (laptop atau ponsel) yang mengakses akun Anda.

b. Jika menemukan perangkat yang bukan milik Anda, klik tiga titik di sebelah kanan, lalu pilih keluar. Ganti password Anda dengan yang lebih kuat.
c. Saat akun Anda telah diretas dan *password* diubah, Facebook akan mengirimkan notifikasi melalui *email* yang Anda daftarkan. Cek apakah ada notifikasi tersebut!
d. Dalam email notifikasi, Facebook menyediakan tautan "Klik di sini" bagi Anda yang tidak membuat perubahan *password* tersebut. Tautan tersebut akan mengarahkan Anda untuk menjawab pertanyaan yang diminta oleh Facebook untuk memulihkan akun Anda.
e. Untuk melaporkan peretasan, klik tautan https://www.facebook.com/hacked.

6. Pengambilalihan Akun Instagram

a. Jika menggunakan laptop, Anda bisa mengetahui apakah ada orang lain yang mengakses akun Anda secara diam-diam dengan mengecek Pengaturan (*setting*) - *Login activity*. Anda akan dibawa pada sebuah halaman yang berisi informasi tentang jenis perangkat dan lokasi *login*.
b. Apabila Anda menemukan adanya perangkat yang tidak Anda gunakan, klik tanda panah di sebelah kanan, lalu klik *logout*.
c. Apabila Anda sudah tidak bisa masuk ke akun Instagram, cek pemberitahuan (*notice*) di alamat email yang Anda daftarkan. Instagram akan mengirimkan pemberitahuan pada setiap perubahan yang terjadi pada akun Instagram Anda, seperti *login* dari perangkat berbeda atau perubahan *password*.
d. Klik fitur *Secure Your Account Here* dan Anda akan dibawa pada halaman untuk mengubah *password*. Masukkan *password* baru yang lebih kuat dan unik.
e. Jika akun sulit dipulihkan, laporkan ke Instagram dengan cara:
    - Pada layar *login*, ketuk "dapatkan bantuan untuk *login*" di bawah fitur *Login* (pada ponsel Android) atau "lupa kata sandi?" pada ponsel IOS.
    - Masukkan nama pengguna, *email*, atau nomor telepon Anda, lalu ketuk "Berikutnya".
    - Ketuk "Perlu bantuan lain?" lalu ikuti petunjuk di layar.
    - Pastikan Anda memasukkan alamat *email* yang aman

dan hanya bisa diakses oleh Anda. Setelah mengirimkan permintaan, tunggu *email* dari Instagram yang berisi langkah berikutnya.

7. Pengambilalihan Akun Tiktok

a. Jika Anda mengalami hal-hal berikut pada akun Tiktok Anda, bisa jadi itu adalah tanda peretasan:
   - Sandi/*password* akun dan nomor telepon yang terhubung telah berubah.
   - *Username* akun atau *nickname* (nama akun) berubah.
   - Video-video yang pernah Anda unggah terhapus atau ada video yang terunggah tanpa izin Anda.

- Akun Anda mengirim pesan tanpa disadari.

b. Laman resmi Tiktok tidak memberitahukan detail prosedur jika pengguna kehilangan akun. Namun, berikut cara yang bisa dilakukan berdasarkan fitur pengamanan yang tersedia pada Tiktok.
   - Buka aplikasi Tiktok pada ponsel, pilih "*forgot password*" atau "lupa *password*".
   - Anda akan diminta memasukkan kontak yang terhubung dengan akun (nomor telepon atau e-mail, tergantung metode pemulihan akun yang pernah dipilih saat pembuatan akun).
   - Pilih tombol "reset" untuk mendapatkan kode pemulihan. Kode pemulihan akan dikirim nomor telepon (via SMS) atau *e-mail*.
   - Masukkan kode tersebut pada menu pemulihan atau "lupa *password*". Jika semua berjalan normal, Anda bisa mengganti sandi dengan yang baru dan lebih kuat.
   - Jika tidak ada masalah, setidaknya peretas tidak dapat mengetahui sandi yang baru. Segera perkuat keamanan akun dengan 2FA yang lebih kuat, misalnya dengan *passkey* fisik jika ada.

c. Hapus perangkat mencurigakan yang terhubung[9]
   - Cek apakah ada yang login akun Tiktok Anda pada perangkat lain.

[9] Tiktok, "My account has been hacked", https://support.tiktok.com/en/log-in-troubleshoot/log-in/my-account-has-been-hacked

- Buka menu "*setting and privacy*" ("pengaturan dan privasi"), lalu pilih "*security*" ("keamanan"). Klik "*select your devices*" ("pilih perangkat").
- Hapus semua perangkat lain yang mencurigakan.
- Penguatan akun dan langkah penghapusan perangkat bisa diakses pada laman *My account has been hacked* pada situs web ofisial Tiktok.

d. Laporkan peretasan ke penyelenggara platform
Langkah-langkah pelaporan masalah ke Tiktok bisa dilihat pada laman *Report a problem* di laman support.tiktok.com atau https://support.tiktok.com/en/log-in-troubleshoot/troubleshooting/report-a-problem.

e. Cari bantuan jika langkah pemulihan gagal
- Tenangkan pikiran, susun kronologi peretasan.
- Dokumentasikan semua tanda peretasan (notifikasi, pemberitahuan pada *e-mail*, dan langkah-langkah pemulihan), misalnya dengan *screenshot* (tangkapan layar).
- Hubungi kontak darurat untuk bantuan penanganan (daftar kontak bantuan penanganan ada di bagian akhir panduan ini).

8. Pengambilalihan Akun Youtube

Setiap akun Youtube terhubung dengan akun Google. Namun, ada kasus saat akun Youtube yang diretas belum bisa pulih kendati akun Gmail telah dipulihkan.

Pada 2022, sebuah akun Youtube milik kelompok aktivis gender minoritas diretas. Peretas mudah mengambil alih akun itu karena kata sandi yang sederhana (mudah ditebak) dan jarang diganti.

Upaya penanganan dilakukan dengan memaksa masuk ke akun Gmail yang terkait akun Youtube tersebut dan bisa kembali dikuasai. Meski demikian, akun Youtube tersebut belum bisa dipulihkan. Setelah melakukan upaya pemulihan berulang, akun Youtube tersebut sudah dihapus.

Muncul e-mail dari Youtube yang memberitahukan bahwa akun tersebut telah dihapus karena dianggap melanggar aturan. Mereka kemudian berulang kali mengajukan banding melalui tautan yang tersedia di e-mail, tetapi Youtube menyatakan akun tersebut tidak lagi terdaftar. Akun baru pulih setelah melaporkan kasus ini ke Google dengan pendampingan dari lembaga yang biasa menangani serangan digital.

a. Mengenali tanda peretasan
   - Muncul perubahan pada akun yang tidak Anda buat. Misalnya perubahan gambar profil, deskripsi, pengaturan *e-mail*, AdSense, atau ada pesan yang terkirim tanpa sepengetahuan Anda.
   - Akun mengunggah video yang tidak pernah Anda buat. Ini berarti ada orang lain yang mengunggah video tersebut dengan akun Google Anda. Cek apakah ada *e-mail* notifikasi yang memperingatkan tentang unggahan video tidak dikenal itu atau adanya aktivitas *login* dari perangkat lain.

b. Pemulihan akun[10]
   1) Pemulihan akun Google/Gmail
      - Jika Anda masih bisa *login* ke akun Google, Segera ganti sandi (*password*) dengan sandi yang lebih kuat, pasang 2FA (dengan aplikasi *authenticator* atau *passkey* fisik).
      - Jika Anda tidak bisa *login* ke akun Google, lakukan langkah pemulihan akun seperti pada poin 3 bagian ini.
      - Lakukan langkah yang sama pada akun-akun Google lainnya.
   2) Jika akun Google bisa diamankan, semestinya akun Youtube bisa kembali dikuasai.
   3) Detail langkah pemulihan akun bisa dilihat pada laman *Recover a hacked* YouTube *channel*.

[10] Google, “Recover a hacked YouTube channel”, https://support.google.com/youtube/answer/76187?hl=en

c. Cari bantuan jika langkah pemulihan gagal
   - Tenangkan pikiran, susun kronologi peretasan.
   - Dokumentasikan semua tanda peretasan (notifikasi, pemberitahuan pada *e-mail*, dan langkah-langkah pemulihan), misalnya dengan *screenshot* (tangkapan layar).
   - Hubungi kontak darurat untuk bantuan penanganan (daftar kontak bantuan penanganan ada di bagian akhir panduan ini).

d. Kembalikan *channel* Youtube ke keadaan sebelum peretasan[11]
   Jika peretas sempat mengambil alih *channel* Youtube, biasanya mereka membuat beberapa perubahan pada *channel* tersebut dan akun Google yang terhubung.
   1) Dokumentasikan semua jejak yang ditinggalkan peretas pada *channel* Youtube tersebut, termasuk pada akun *e-mail* yang terhubung. Salah satu caranya adalah dengan menyimpannya pada situs pengarsipan seperti https://perma.cc/ atau https://archive.is/.

   2) Hapus semua pengguna yang terhubung dengan *channel* Youtube tersebut.
      - Jika menggunakan "*channel permissions*", masuklah (*sign in*) ke YouTube Studio. Klik "*Setting", "Permissions*". Pilih username yang hendak dihapus. Klik "*Remove access*".
      - Jika menggunakan "*brand account*", masuklah ke bagian "*Brand Accounts*" pada pengaturan Google Account. Ikuti prosedur penghapusan yang serupa dengan yang di atas.

   3) Mengembalikan *channel* ke pengaturan awal.
      Jika peretas mengubah nama *channel*, gambar profil, dan banner, lakukan perubahan ke status awal untuk menghindari penghapusan akun secara permanen.

   4) Hapus video-video yang diunggah oleh peretas secara permanen.

[11] Google, "Clean up a hacked YouTube channel", https://support.google.com/youtube/answer/14849770#zippy=%2Cdelete-hacker-uploaded-videos-without-violations%2Crestore-your-channels-basic-info-and-branding%2Cremove-any-unknown-users-from-your-channel-or-account

5) Detail petunjuk upaya pemulihan akun hingga pengembalian pengaturan channel bisa dibaca pada laman *Clean up a hacked YouTube channel*.

C. Serangan Pendengung (Buzzer)

Ada berbagai bentuk serangan yang dilakukan *buzzer*, seperti *trolling* (menciptakan kekacauan melalui komentar, argumen, atau informasi palsu untuk memancing reaksi negatif), *doxing* (pengungkapan identitas pribadi seseorang yang menjadi target), *impersonating* (peniruan/pemalsuan akun), hingga kekerasan berbasis gender *online* (KBGO).

Berikut beberapa langkah merespons serangan yang diadopsi dari Bab 6 Panduan Keamanan Digital untuk Jurnalis 2022 .

a. Doxing

- Jika terjadi alamat rumah awak media diungkap, perusahaan media perlu mencari rumah aman sementara bagi korban dan keluarga hingga serangan mereda.
- Laporkan postingan yang mengandung *doxing* ke platform dan blokir akun pelaku.
- Jika pelaku mengungkap nomor telepon dan korban menerima banyak gangguan, telepon perlu dimatikan sementara waktu dan pertimbangkan mengganti nomor telepon di kemudian hari.
- Jika pelaku mengekspos nomor rekening bank, kartu kredit, atau informasi akun keuangan korban lainnya, segera hubungi semua lembaga keuangan yang terlibat dan laporkan pelanggarannya.
- Menutup sementara akun media sosial menjadi pilihan terbaik jika serangan meningkat.
- Laporkan ke polisi atas *doxing* dengan membawa hasil dokumentasi dan tautan.
- Arsipkan melalui https://perma.cc/ atau https://archive.is/.

b. Impersonating
   - Buat pengumuman tentang pemalsuan akun agar publik (audiens dan *followers*) tidak tertipu.
   - Laporkan akun yang menggunakan identitas media atau awak media Anda ke penyedia platform agar akun palsu tersebut ditutup.
   - Pelaporan akun palsu di Facebook: https://s.id/akunpalsuFB
   - Pelaporan akun palsu di Twitter atau X: https://help.x.com/en/forms/authenticity/impersonation
   - Pelaporan akun palsu di Instagram: https://s.id/akunpalsuIG
   - Pelaporan akun palsu Gmail: https://s.id/akunpalsuGmail

c. Pelecehan *Online* dan KGBO
   - Laporkan/blokir akun, postingan atau komentar yang mengandung pelecehan termasuk KBGO ke platform.
   - Minta dukungan dari organisasi profesi atau lembaga penyedia layanan pendamping pelecehan/kekerasan seksual.
   - Laporkan ke polisi atas kekerasan dan pelecehan yang diterima korban, baik melalui telepon, sms, *chat*, atau di media sosial lainnya dengan menyertakan dokumentasi kekerasan/ pelecehan yang dialami.
   - Perusahaan media memfasilitasi layanan pemulihan trauma awak media yang menjadi korban.

BAB VIII
Panduan Keamanan Digital Organisasi Lain

Perusahaan media juga dapat mempelajari dan mengadopsi panduan keamanan digital yang diterbitkan organisasi lain. Tentu perlu disesuaikan dengan kebutuhan masing-masing perusahaan media. Berikut ini panduan keamanan digital dari organisasi lain yang bisa memperkaya panduan digital perusahaan media

1. https://gijn.org/digital-security/
2. https://cpj.org/2019/07/digital-safety-kit-journalists.php#protect
3. https://digitalrightswatch.org.au/2019/06/10/digital-security for-journalists/
4. https://cpj.org/2020/05/digital-safety-protecting-against targeted-online-attacks/
5. https://coconet.social/digital-hygiene-safety-security-indonesia/
6. https://freedom.press/training/your-smartphone-and-you handbook-modern-mobilemaintenance/
7. https://www.accessnow.org/issue/digital-security/
8. https://digitalfirstaid.org/en/index.html
9. https://securityinabox.org/en/guide/basic-security/android/
10. https://id.safenet.or.id/wp-content/uploads/2019/11/Panduan KBGO-v2.pdf
11. https://digsec.safenet.or.id

BAB IX
Kontak Darurat

A. Kontak Bantuan Penanganan

Dalam situasi terjadi serangan atau saat media membutuhkan langkah-langkah mitigasi, berikut ini lembaga-lembaga yang bisa dikontak untuk memberikan bantuan.

1. Aliansi Jurnalis Independen (AJI)
   Link pengaduan: https://safetycorner.aji.or.id/node/6511
2. Tim Reaksi Cepat (TRACE)
   Link pengaduan: https://lapor.trace.mu/
3. SAFEnet
   Link pengaduan: https://aduan.safenet.or.id/
4. Access Now
   Link pengaduan: https://www.accessnow.org/help/#contact-us

B. Kontak Bantuan Hukum

a. Kontak-kontak bantuan hukum

Wilayah Jabodetabek

Lembaga	Alamat	Telepon	Faks	Email
LBH Pers	Jl. Kalibata Timur IV G No.10 Kalibata, Pancoran, Jakarta Selatan	021-79183485, 0821-4688-8873		secretariat@l bhpers.org
YLBHI	Jl. Diponegoro No.74, Menteng, Jakarta Pusat 10320	021-3929840	021-31930140	info@ylbhi.or.id
LBH Jakarta	Jl. Pangeran Diponegoro No.74, Menteng, Jakarta 10320	021-3145518	021-3912377	lbhjakarta@bantuanhukum.or.id
PBHI	Jl. Hayam Wuruk No.4, RT.9/RW.5, Kb. Klp., Kec. Taman Sari, Jakarta 10120	021-3859968		
LBH Apik Jakarta	Jl. Raya Tengah No. 31 RT01 RW09 Kampung Tengah Kramat Jati Jakarta Timur 13540	021–87797289, 0813-888226699	021–87793300	LBHAPIK@gmail.com

Wilayah Jawa Barat dan Banten

Lembaga	Alamat	Telepon	Faks	Email
LBH Bandung	Jl. Kalijati Indah Barat No 8, Antapani, Bandung	0821-2017-1321		konsultasi@lbhbandung.or.id
LBH Apik Jabar	Jl. Beringin No.9 Kemiri Muka, Beji, Kota Depok, Jawa Barat	0813-8030-4852		lbhapikjawabarat@gmail.com
LBH Apik Banten	Jl. Raya Pandeglang Km. 3, Komp. Tembong Indah, Sempu, Kota Serang – Banten	0254-227969	0254-227969	

Wilayah Jawa Tengah dan DIY

Lembaga	Alamat	Telepon	Faks	Email
LBH Semarang	Jl. Jomblangsari 4 No. 17, Jomblang, Candisari, Kota Semarang	024-86453054, 0882-2890-2001		office.lbhsemarang@ylbhi.or.id
LBH Apik Semarang	Jl. Poncowolo Timur Raya No. 455 Semarang,Jawa Tengah (masuk melalui jalan Indraprasta)	024-3510499	021-31930140	apiksemarang@yahoo.com
LBH Yogyakarta	Jl. Benowo No.309, Winong, RT 12/ RW 03, Prenggan, Kec. Kotagede, Kota Yogyakarta, Daerah Istimewa Yogyakarta 55172	0274-4351490	021-3912377	kalabahulbhjogja@gmail.com
LBH Apik Yogyakarta	Jl. Nogodewo 12, Gowok, Sleman, Yogyakarta	0274-379614, 08179410624	021–87793300	apik_jogja@yahoo.com

Wilayah Jawa Timur

Lembaga	Alamat	Telepon	Faks	Email
LBH Surabaya	Jl. Kidal No.6, Pacar Keling, Kec. Tambaksari, Kota SBY, Jawa Timur 60131	031-5022273		bantuanhuku msby@gmail.com
LBH Surabaya Pos Malang	Jl. Teluk Perigi Rt 01, Rw 10 Tirtomoyo, Kec. Pakis, Kab. Malang, Jawa Timur 65154	081252226205		lbhmalang@ylbhi.or.id
LBH APIK-Kota Batu	Jl. Kapten Ibnu, Ruko 8 RT03/ RW13, Kel Sisir, Batu, Kota Batu, Jawa Timur	6281336554420		lbhapikkotabatu@gmail.com

Wilayah Bali dan Nusra

Lembaga	Alamat	Telepon	Faks	Email
LBH Bali	Jl. Plawa No.57, Denpasar Timur, Denpasar, Bali	0361-223010		lbhbali@indo.net.id
LBH APIK Bali	Jl. Suli 119 – A3, Denpasar Timur	0361–9272245, 081337325896		lbh.tentrem@gmail.com
LBH APIK NTT	Jl. Sam Ratulangi II no.33B Walikota Baru, Kel. Oesapa Barat, Kec. Kelapa Lima, Kota Baru, Kupang 85228.	0380 823647		lbhapik.ntt@gmail.com
LBH APIK NTB	Jl. Angklung Raya no. 2 Karang Bedil, Mataram, Lombok, NTB	0817-5768-496, 0823-3959-3221		lbhapikntb17@gmail.com

Wilayah Aceh dan Sumatera Utara

Lembaga	Alamat	Telepon	Faks	Email
LBH Banda Aceh	Jl. Sakti Lorong LBH Banda Aceh No.1, Desa Pango Raya, Ulee Kareng, Banda Aceh 23119	0651-8057952		lbh_aceh1995@yahoo.com
LBH APIK Aceh	Jl. Tengku Daud No. 147, Panggoi, Muara Dua, Kota Lhoksmeumawe, Aceh 24355	0645-43150		lbhapikaceh@gmail.com
LBH Medan	Jl. Hindu No.12 Medan 20111, Sumatera Utara, Indonesia	061-4515340	061-4569749	lbh_medan@ yahoo.com, kantor@lbhm edan.org
LBH APIK Medan	Jl. Jermal V No. 1C, Denai, Medan Denai	0821-5753-9308, 0282-115063359		admlbhapikm edan@gmail.com

Wilayah Sumatera Barat dan Riau

Lembaga	Alamat	Telepon	Faks	Email
LBH Padang	Jl. Pekanbaru No 11A, Kota Padang, Sumatra Barat	0751-7056059		
LBH Pekanbaru	Jl. Sapta Taruna No.51, Tengkerang Utara, Kec. Bukit Raya, Kota Pekanbaru, Riau 28289	0761-45832, 0811-765-832		info@lbhpeka nbaru.or.id

Wilayah Sumatera Selatan dan Lampung

Lembaga	Alamat	Telepon	Faks	Email
LBH Palembang	JL. HBR Motik No.12A Rt.29 Rw.9 Kel.Karya Baru Kec. Alang-alang Lebar Kota Palembang	0711-5610122, 0813-6930-0442		lbhpalembang@ylbhi.or.id
LBH APIK Sumatera Selatan	Jl. Sekip Bendung Dalam No.009 RT. 035 RW. 009, Kel. 8 Ilir, Kec. Ilir Timur III, Kota Palembang	0821-7770-0069		yayasanlbhapiksumsel@gmail.com
LBH Bandar Lampung	Jl. Sam Ratulangi, Gg Mawar 1, Nomor 7, Gedong Air, Bandar Lampung 351117	0721-5600425		bantuanhukumlampung@gmail.com

Wilayah Kalimantan

Lembaga	Alamat	Telepon	Faks	Email
LBH Kalimantan Barat	Jl. Dr. Sutomo, Komplek Batara Indah 4 No. 16 D, Pontianak, Kalimantan Barat	0812-5880-6816		lbhkalbar@ylbhi.or.id
LBH APIK Pontianak	Jl. Alianyang No. 12A Pontianak, Kalimantan Barat 78116	0561–766439		apik_ptk@ya hoo.com
LBH Samarinda	Jl. Wijaya Kusuma II No 50, Air Putih, Samarinda Ulu Samarinda	0821-5133-15537		lbhsamarinda @ylbhi.or.id, lbhsamarind @gmail.com
LBH APIK Kalimantan Timur	Jl. Sultan Sulaiman, Perum Citra Gading Blok B2 No. 9 Samarinda – Kalimantan Timur	0541-4106482, 0812-5822-715, 0812-5826-828		ylbhapikkalti m@gmail.com
LBH Palangka Raya	Jl. Parawei, Perum Casadova blok B, No. 10, Kota Palangka Raya, Prov. KalimantanTengah	0857-8696-8317		ylbhi.lbh.palangkaraya@gmail.com

Wilayah Sulawesi dan Papua

Lembaga	Alamat	Telepon	Faks	Email
LBH Manado	Jl. A Manonutu No. 29, Wanea, Kota Manado 95116	0431-8806473, 085256303949, 085240523068		secretariat@l bhpers.org
LBH APIK Manado	Jl. Bethesda 6 No. 77, Ranotanaling II, Manado - 95116	0431-824132	021-31930140	info@ylbhi.or.id
LBH Makassar	Jl. Nikel 1 Blok A22 No.18 Kota Makassar, Kode Pos 90222	0411-4677699	021-3912377	lbhjakarta@bantuanhukum.or.id
LBH APIK Makassar	Jl. Perintis Kemerdekaan, Perum Budidaya Permai Blok D no. 3, Makassar, Sulawesi Selatan			
LBH APIK Palu	Jl. Teluk Tomini No. 8B, Kota Palu - 94221	0451-4015986, 0811-4540-1616	021–87793300	LBHAPIK@gmail.com
LBH Papua	Jl. Gerilyawan No. 46 Jayapura, Papua 99532	0967-581710, 08124808635		
LBH APIK Jayapura	Jl. Raya Sentani, Padang Bulan, Abepura, Jayapura, Papua 99351	0411-590147, 0812-9400-7696		

C. Kontak Penanganan Psikososial

1. Yayasan Pulih
   Alamat: Jl. Teluk Peleng 63 A Komplek AL-Rawa Bambu Pasar Minggu Jakarta 12520
   Telepon: 021-788 42 580, 021- 982 86 39
   E-mail: pulihfoundation@gmail.com; pulihcounseling@gmail.com
2. Jaringan LBH Apik di berbagai kota

