P3IK:

Pertolongan Pertama Pada Insiden Keamanan

MODUL PENANGANAN
INSIDEN KEAMANAN UNTUK PPHAM DAN OMS

kemitraan partnership
SAFEnet

P3IK: Pertolongan Pertama Pada Insiden Keamanan

MODUL PENANGANAN
INSIDEN KEAMANAN UNTUK PPHAM DAN OMS

September 2024

Tim Penyusun
Koordinator
Nenden Sekar Arum

Penulis
Adi
Fani
Kimberly

Editor
Aseanty Pahlevi

Desain & Tata Letak
Atsarina Kardina

Penafian
Publikasi Kertas Kebijakan ini dihasilkan dengan dukungan dana dari Kemitraan bagi Pembaruan Tata Pemerintahan di Indonesia. Materi dalam publikasi ini adalah semata-mata tanggung jawab dari SAFEnet dan tidak otomatis mencerminkan pandangan dari KEMITRAAN.

Diterbitkan oleh
Southeast Asia Freedom of Expression Network (SAFEnet)
Jalan Gita Sura III Nomor 55 Peguyangan Kaja,
Denpasar, Bali 80115
+62 811 9223375

info@safenet.or.id
@safenetvoice
safenet.or.id



Laporan ini menggunakan lisensi Creative Commons Attribution-NonCommercial 4.0 (CC BY-NC 4.0). Anda bebas untuk untuk mendistribusikan, mencampur ulang, mengadaptasi, dan membuat materi dalam media atau format apa pun hanya untuk tujuan nonkomersial, dan hanya selama atribusi diberikan kepada pencipta. Informasi lebih lanjut di https://creativecommons.org/licenses/by- nc/4.0/

Daftar Isi

Kata Pengantar

Psikososial

- a. Keamanan dan Konteks Kita 07
- b. Mengenal Trauma dan Pertolongan Pertama Psikososial 09
- c. Pertolongan Pertama pada Kasus Kekerasan Seksual 13

Keamanan Digital

- a. Empat Tahap Penanganan Insiden Digital 16
- b. Langkah Penanganan: Doxxing 19
- c. Langkah Penanganan: Akun Diambil Alih 22
- d. Langkah Penanganan: Peranti Mobile 24

Keamanan Fisik

- a. Kesadaran Situasional 29
- b. Pendekatan Bertahap untuk Mengelola Risiko 36
- c. Keamanan Tempat Kerja 40
- d. Surveillance/Pengawasan 45
- e. Penahanan vs. Penangkapan 47
- f. Mengikuti atau Meliput Demonstrasi dan Protes 48

Kata Pengantar

Perkembangan teknologi dan informasi yang begitu pesat telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia. Di satu sisi, kemajuan ini memberikan berbagai kemudahan dan memperluas akses masyarakat dalam berbagai aktivitas, mulai dari interaksi sosial hingga pekerjaan sehari-hari. Namun, di sisi lain, kemajuan ini juga memunculkan berbagai tantangan baru, termasuk peningkatan kejahatan digital seperti penipuan online, pencurian data, dan Kekerasan Berbasis Gender Online (KBGO).

Kemajuan teknologi telah membuka ruang baru bagi serangan terhadap kelompok-kelompok kritis, termasuk Pembela Hak Asasi Manusia (PPHAM), aktivis, jurnalis, dan organisasi masyarakat sipil (OMS). Dalam konteks Indonesia, serangan terhadap kebebasan sipil, baik secara offline maupun online, terus terjadi. Data dari Southeast Asia Freedom of Expression Network (SAFEnet) menunjukkan bahwa serangan digital yang menyasar kelompok kritis semakin meningkat, dengan serangan terhadap PPHAM, terutama perempuan, menjadi perhatian utama.

Untuk menghadapi tantangan ini, diperlukan respons yang terstruktur dan menyeluruh, baik dari individu maupun organisasi. Oleh karena itu, SAFEnet, didukung oleh KEMITRAAN melalui Program ELEVATE, berkomitmen untuk meningkatkan kapasitas Organisasi Masyarakat Sipil dalam menangani insiden keamanan, khususnya yang menimpa PPHAM.

Melalui penyusunan modul dan kurikulum pelatihan ini, diharapkan akan tercipta lebih banyak individu dan organisasi yang mampu menangani insiden keamanan holistik di berbagai daerah di Indonesia. Dengan begitu, kita bersama-sama dapat menciptakan lingkungan yang lebih aman dan terlindungi bagi para PPHAM dan seluruh elemen masyarakat sipil di Indonesia.

Kami berharap modul ini dapat menjadi panduan yang bermanfaat dalam upaya kolektif kita untuk menangani dan mencegah insiden keamanan dengan pendekatan holistik, serta melindungi hak asasi manusia di era digital ini.

Denpasar, September 2024

Nenden Sekar Arum
Direktur Eksekutif
Southeast Asia Freedom of Expression Network (SAFEnet)

// P3IK: Pertolongan Pertama Pada Insiden Keamanan
Modul Penanganan Insiden Keamanan untuk PPHAM dan OMS

PSIKOSOSIAL



01

A. Keamanan dan Konteks Kita

Keamanan holistik adalah pendekatan yang mencakup berbagai aspek perlindungan untuk memastikan kesejahteraan individu secara keseluruhan. Pendekatan ini mencakup keamanan psikososial, keamanan digital, dan keamanan fisik. Dalam aspek psikososial, mencakup perlindungan terhadap upaya menjaga kesehatan mental dan emosional seseorang. Upaya ini termasuk dukungan untuk menghadapi stres, trauma, dan tekanan kerja.

Aspek Keamanan digital berfokus terhadap upaya melindungi informasi pribadi dan profesional dari ancaman online, seperti peretasan, pencurian data, dan serangan siber. Sedangkan keamanan fisik melibatkan langkah-langkah untuk melindungi diri dari ancaman fisik, seperti kekerasan, penyerangan, dan bahaya lingkungan.

Mengetahui dan menerapkan keamanan holistik sangat penting karena memberikan pendekatan yang komprehensif untuk perlindungan, yang tidak hanya fokus pada satu aspek keamanan saja. Ini membantu individu dan organisasi dalam menghadapi berbagai ancaman dan tekanan yang mungkin mereka hadapi dalam kehidupan sehari-hari, baik di dunia nyata maupun di dunia digital.

Dengan demikian, keamanan holistik memastikan bahwa kesejahteraan individu terlindungi dari berbagai sudut,

// Aspek Keamanan digital berfokus terhadap upaya melindungi informasi pribadi dan profesional dari ancaman online, seperti peretasan, pencurian data, dan serangan siber.



memungkinkan mereka untuk berfungsi lebih efektif dan merasa lebih aman dalam menjalankan tugas dan tanggung jawab mereka.

Keamanan holistik dan interseksionalitas saling terkait dalam memahami dan menangani berbagai aspek kerentanan yang dihadapi individu dan kelompok. Keamanan holistik mencakup pendekatan menyeluruh terhadap perlindungan fisik, psikososial, dan digital, yang memperhitungkan kebutuhan dan tantangan individu secara keseluruhan.

Interseksionalitas adalah konsep yang menekankan bahwa berbagai identitas sosial dan politik, seperti ras, gender, kelas, dan orientasi seksual, saling berinteraksi dan memengaruhi pengalaman individu terhadap penindasan dan diskriminasi.

Hubungan antara keduanya adalah sebagai berikut:

1. *Pendekatan Komprehensif: Keamanan holistik mengakui bahwa ancaman terhadap keamanan seseorang tidak hanya datang dari satu sumber, tetapi bisa berasal dari berbagai aspek kehidupan. Interseksionalitas memperkuat pemahaman ini dengan menunjukkan bagaimana berbagai identitas dan pengalaman seseorang mempengaruhi tingkat kerentanan mereka terhadap ancaman tersebut.*

2. *Konteks Sosial yang Kompleks: Interseksionalitas membantu mengidentifikasi bagaimana faktor-faktor sosial yang kompleks dan saling terkait mempengaruhi pengalaman individu. Dengan demikian, pendekatan keamanan holistik yang mempertimbangkan interseksionalitas dapat lebih efektif dalam merespons kebutuhan keamanan yang spesifik dan berbeda dari setiap individu atau kelompok.*

3. *Kebijakan dan Praktik yang Adil: Pendekatan holistik terhadap keamanan yang mempertimbangkan interseksionalitas membantu dalam merancang kebijakan dan praktik yang lebih adil dan inklusif. Ini memastikan bahwa perlindungan diberikan dengan mempertimbangkan berbagai bentuk diskriminasi dan ketidakadilan yang mungkin dihadapi oleh individu berdasarkan identitas mereka yang beragam.*

4. *Pencegahan dan Intervensi yang Tepat: Dengan memahami bagaimana identitas yang berlapis-lapis dapat meningkatkan kerentanan, intervensi keamanan dapat disesuaikan untuk lebih efektif mencegah dan menangani ancaman. Misalnya, seorang perempuan dari komunitas minoritas mungkin menghadapi ancaman yang berbeda dan lebih kompleks dibandingkan dengan perempuan dari kelompok mayoritas, sehingga memerlukan pendekatan yang lebih disesuaikan.*

Keamanan holistik yang mempertimbangkan interseksionalitas mampu memberikan perlindungan yang lebih tepat, inklusif, dan efektif, karena memperhitungkan kerentanan dan kebutuhan individu yang beragam berdasarkan identitas mereka yang beragam.

B. Mengenal Trauma dan Pertolongan Pertama Psikososial

Memahami trauma sangat penting karena banyak profesi, seperti jurnalis dan pembela HAM, seringkali terpapar pada peristiwa traumatis. Penelitian menunjukkan bahwa antara 80 hingga 100% jurnalis mengalami peristiwa traumatis terkait pekerjaan mereka. Trauma tidak hanya berdampak pada kesehatan mental tetapi juga dapat mempengaruhi sikap, perilaku, dan fungsi seseorang secara keseluruhan. Trauma adalah setiap pengalaman yang mengganggu yang menyebabkan rasa takut signifikan, ketidakberdayaan, disosiasi, kebingungan, atau perasaan mengganggu lainnya yang cukup kuat untuk memiliki efek negatif jangka panjang.

Jenis-jenis Trauma

Trauma dapat disebabkan oleh berbagai jenis peristiwa, baik yang disebabkan oleh perilaku manusia maupun oleh alam. Berikut adalah beberapa contoh jenis trauma:

1. *Peristiwa yang Menimbulkan Stres: Kematian, kedukaan, bunuh diri, kecelakaan, dan cedera.*
2. *Sumber Stres dari Organisasi/Kantor: Perundungan, ancaman, pengkhianatan, kejahatan, isolasi ekstrem, tekanan kronis, konflik yang belum terselesaikan, lingkungan kerja yang tidak sehat, beban kerja yang berat.*
3. *Stresor Fisik: Kebisingan, lingkungan yang kacau, rasa tidak ada kendali atas ruang, ketakutan akan keamanan fisik, lampu yang terlalu terang atau berkedip, suhu ekstrem, bekerja di tengah konstruksi.*
4. *Ancaman Eksternal: Evakuasi, lockdown, kebakaran, perampokan, kekerasan fisik atau ancaman kekerasan fisik, penyerangan fisik atau seksual.*

Refleksi dalam Menanggapi Trauma

Saat menghadapi trauma yang dialami orang lain, penting untuk menerapkan prinsip *"Do No (More) Harm."* Artinya, kita harus berhati-hati agar tidak menyebabkan kerusakan lebih lanjut. Sebagai individu yang bukan profesional kesehatan mental, penting untuk menyadari kapasitas dan keterbatasan diri. Transparansi tentang keahlian dan latar belakang juga penting dalam berinteraksi dengan orang yang mengalami trauma.

Cara Menanggapi Trauma

Diskusi Aman tentang Peristiwa Traumatis

1. ***Empati dan Kasih Sayang:***
   Tanggapi dengan empati dan kasih sayang, tetapi hindari simpati yang dapat memperburuk situasi.

2. ***Aktif Mendengarkan:***
   Praktikkan mendengarkan secara aktif, di mana fokusnya adalah mendengarkan dengan penuh perhatian tanpa menghakimi. Tujuannya adalah untuk memahami perspektif orang lain dan menyampaikan kembali bahwa Anda memahami mereka.

3. ***Komunikasi Nonverbal:***
   Tampilkan kesadaran dan ketertarikan terhadap apa yang dikomunikasikan baik secara verbal maupun nonverbal.

Keterampilan Mendengar Aktif

Keterampilan mendengar aktif adalah elemen penting dalam menangani trauma. Berikut adalah beberapa teknik

1. ***Mendengar Aktif:***
   Mendengarkan baik-baik tanpa menghakimi atau mengevaluasi untuk memahami perspektif orang lain.

2. ***Parafrase:***
   Mengemukakan kembali apa yang dikatakan dengan kata-kata yang berbeda dan lebih singkat tanpa mengubah maknanya. Ini memastikan bahwa pendengar menangkap informasi dan maksud yang sama.

3. ***Merefleksikan:***
   Mencerminkan kembali perasaan atau emosi di balik perkataan seseorang. Ini membantu memastikan bahwa Anda memahami apa yang dirasakan orang lain.

4. ***Merangkum:***
   Membuat ringkasan atau kesimpulan dari poin-poin utama pernyataan yang disampaikan. Misalnya, "Dari awal sampai apa yang Anda sampaikan barusan, dapat saya simpulkan..."

mendengar aktif yang dapat dilakukan:

Kunci: Empati dan Apresiasi

• Definisi Empati

Empati adalah tindakan memahami, menyadari, dan peka terhadap perasaan, pikiran, dan pengalaman orang lain. Ini melibatkan perasaan seolah-olah kita berada dalam posisi orang lain. Dalam konteks menanggapi trauma, penting untuk menormalisasi reaksi yang dialami orang dan menyampaikan bahwa ada orang lain yang juga mengalami hal yang sama.

Empati berbeda dengan simpati. Simpati menekankan sudut pandang sendiri, sedangkan empati menempati sudut pandang orang lain menemukan perspektif orang lain.

• Apresiasi

Menghargai keberanian orang dalam berbagi pengalaman traumatis sangat penting. Contoh-contoh respon mendukung bisa berupa pernyataan seperti, "Terima kasih sudah berbagi dengan kami," atau "Terima kasih sudah mempercayai saya, pasti tidak mudah untuk menceritakan pengalaman yang Anda alami.

Contoh Respon Mendukung

• Menggunakan Pertanyaan Terbuka

Pertanyaan terbuka membantu mengeksplorasi perasaan, pikiran, dan respon orang. Pertanyaan ini membutuhkan lebih dari satu kata tanggapan, seperti "Bagaimana?" atau "Apa yang terjadi?" Mendengarkan lebih banyak daripada berbicara adalah kunci, dan penting untuk berhati-hati dengan pertanyaan "kenapa" yang bisa terkesan menyalahkan. Sebaiknya ganti dengan "Apa yang membuat Anda..."

• Nada Suara dan Sikap

Menjaga nada suara agar tidak terlalu tinggi dan cenderung rendah membantu menciptakan lingkungan yang aman dan mendukung.

Teknik Mengatasi Reaksi Emosional

• Teknik Grounding

Teknik grounding digunakan untuk membantu meredakan reaksi emosional yang intens. Beberapa teknik yang disarankan dalam dokumen termasuk pernapasan 4-7-8, metode 54321, genggam jari, dan butterfly hug. Melakukan teknik-teknik ini bersama-sama dapat membantu menenangkan dan menstabilkan emosi.

Video: https://www.youtube.com/watch?v=718uW3_1GlE

• Koregulasi

Koregulasi melibatkan menenangkan dan mengelola respon emosional melalui dukungan dari individu lain yang terhubung. Teknik bicara dan strategi relaksasi serta stabilisasi emosi juga digunakan dalam koregulasi.

Mengenal Pertolongan Dasar Psikososial (PFA)

Pertolongan Dasar Psikososial atau Psychosocial First Aid (PFA) adalah pendekatan yang dirancang untuk

memberikan bantuan segera kepada individu yang mengalami trauma atau stres berat akibat krisis atau bencana. PFA bertujuan untuk mengurangi tekanan awal yang dialami oleh individu dan memfasilitasi adaptasi jangka panjang yang lebih baik. Ini bukan terapi profesional tetapi lebih merupakan langkah pertama dalam memberikan dukungan psikologis dasar dan menghubungkan individu dengan sumber daya yang diperlukan.

Prinsip 3L dalam PFA

Prinsip 3L dalam PFA terdiri dari tiga langkah utama yang harus diikuti ketika memberikan pertolongan dasar psikososial:

1. ***Look (Lihat):***
   Mengamati situasi dan mengidentifikasi individu yang membutuhkan bantuan. Ini termasuk memperhatikan tanda-tanda distress atau trauma, seperti perilaku yang berubah, ekspresi wajah, dan reaksi fisik.

2. ***Listen (Dengarkan):***
   Mendengarkan dengan empati dan tanpa menghakimi apa yang disampaikan oleh individu yang mengalami trauma. Hal ini penting untuk membangun rasa percaya dan memberikan ruang bagi mereka untuk mengungkapkan perasaan dan pengalaman mereka.

4. ***Link (Hubungkan):***
   Menghubungkan individu dengan dukungan lebih lanjut dan sumber daya yang tersedia, seperti layanan kesehatan mental, dukungan komunitas, atau bantuan profesional lainnya. Ini memastikan bahwa individu mendapatkan bantuan yang mereka butuhkan untuk proses pemulihan jangka panjang.

Apa Saja yang Boleh dan Tidak Boleh Dilakukan Ketika PFA?

Yang Boleh Dilakukan:

1. Dekati dengan Hati-Hati: Pastikan pendekatan Anda tidak menambah tekanan atau ketakutan pada individu.
2. Stabilisasi Emosi: Bantu individu menenangkan diri dan mengelola reaksi emosional mereka.
3. Tunjukkan Empati: Berikan dukungan dengan sikap empatik dan penuh pengertian.
4. Validasi Perasaan: Akui dan hormati perasaan mereka, biarkan mereka tahu bahwa apa yang mereka rasakan adalah wajar.
5. Bagikan Informasi yang Relevan: Berikan informasi yang dapat membantu mereka memahami situasi dan langkah-langkah selanjutnya.
6. Tetap Hargai Privasi: Jaga kerahasiaan informasi pribadi dan pastikan mereka merasa aman.

Yang Tidak Boleh Dilakukan:

1. Jangan Menghakimi: Hindari memberikan penilaian atau kritik terhadap perasaan atau reaksi mereka.

2. Jangan Memaksa untuk Bicara: Jika mereka tidak siap untuk berbicara, jangan memaksa. Berikan waktu dan ruang bagi mereka.

3. Jangan Memberikan Janji Palsu: Jangan menjanjikan sesuatu yang tidak dapat Anda penuhi, ini dapat merusak kepercayaan.

4. Jangan Memberikan Simpati Berlebihan: Simpati yang berlebihan dapat membuat mereka merasa lebih lemah atau tidak berdaya.

5. Jangan Mengabaikan: Jangan abaikan tanda-tanda distress yang jelas, pastikan untuk memberikan perhatian yang cukup.

6. Hindari Bahasa yang Menyalahkan: Gunakan bahasa yang mendukung dan hindari pertanyaan yang terkesan menyalahkan.

Dengan memahami dan menerapkan PFA serta prinsip 3L, kita dapat memberikan bantuan yang efektif dan tepat kepada individu yang mengalami trauma, membantu mereka merasa didukung dan dipahami, serta mengarahkan mereka pada bantuan lebih lanjut yang mereka butuhkan.

C. Pertolongan Pertama pada Kasus Kekerasan Seksual

Dokumen "Pertolongan Pertama pada Kasus Kekerasan Seksual" menyediakan panduan komprehensif untuk memberikan bantuan awal kepada korban kekerasan berbasis gender dan seksual. Pertolongan pertama psikososial (PFA) ini sangat penting dalam merespons situasi krisis dengan cara yang empatik dan efektif. Langkah-langkah yang diuraikan dalam dokumen ini memberikan kerangka kerja bagi individu dan organisasi untuk mendukung korban secara menyeluruh.

Langkah Pertama: Respon Awal

Ketika seseorang melaporkan mengalami pelecehan atau kekerasan seksual, hal pertama yang harus dilakukan adalah memastikan keselamatan korban dan mendengarkan mereka dengan empati tanpa menghakimi. Penting untuk meyakinkan korban bahwa mereka tidak sendirian dan bahwa bantuan tersedia. Informasi dasar yang perlu diketahui mencakup:

- Gender korban
- Usia korban
- Lokasi kejadian
- Gambaran singkat tentang peristiwa yang terjadi
- Kebutuhan dasar yang harus segera ditanggapi, seperti rumah aman, psikolog, atau tindakan untuk takedown akun online.

Langkah-Langkah Pertolongan Pertama:

1. Kasus Perkosaan:

- Simpan Barang Bukti: Penting untuk menyimpan semua bukti yang ada seperti pesan chat dan pakaian yang dikenakan saat kejadian.
- Jangan Mandi: Jika korban ingin melapor ke kepolisian, sebaiknya jangan mandi terlebih dahulu untuk menjaga keutuhan bukti fisik.
- Kunjungi Rumah Sakit: Korban bisa meminta rekaman medis sebagai bukti tambahan. Ini penting meskipun korban belum siap untuk menjalani visum.
- Kontrasepsi Darurat: Jika diperlukan, pertimbangkan penggunaan kontrasepsi darurat (morning after pills) untuk mencegah kehamilan yang tidak diinginkan.

2. Kasus Kehamilan Tidak Direncanakan (KTD):

- Tanya Kondisi dan Situasi Korban: Menggali lebih dalam mengenai situasi dan kondisi korban dengan cara yang sensitif.
- Tanyakan Usia Kehamilan: Jika korban nyaman, tanyakan sudah berapa bulan kehamilannya.
- Cari Tahu Keinginan Korban: Apakah korban ingin mempertahankan kehamilan, melakukan aborsi, atau mengadopsi anak tersebut.
- Jelaskan Pilihan yang Ada: Sampaikan opsi yang tersedia seperti mempertahankan kehamilan, aborsi, atau adopsi.
- Akses Konseling: Hubungi layanan konseling untuk memberikan dukungan lebih lanjut kepada korban.

3. Kasus Kekerasan Berbasis Gender Online (KBGO):

- Simpan Bukti Kekerasan Online: Dokumentasikan semua bukti kekerasan yang terjadi secara online.
- Dokumentasikan Link: Jika video atau foto sudah tersebar, dokumentasikan link tersebut sebagai bukti.
- Ganti Password: Jika akun korban terkena serangan, segera ganti password untuk mencegah akses lebih lanjut.
- Kontak Layanan Takedown: Hubungi layanan untuk takedown posting seperti awasKBGO, Taskforce KBGO, atau Srikandi KBGO untuk menghapus konten yang merugikan.

// P3IK: Pertolongan Pertama Pada Insiden Keamanan
Modul Penanganan Insiden Keamanan untuk PPHAM dan OMS

KEAMANAN DIGITAL



02

A. Empat Tahap Penanganan Insiden Digital

Dalam menangani insiden digital, umumnya terdapat empat tahapan, yaitu:

1. ***Tahap 1:*** *Persiapan*
2. ***Tahap 2:*** *Deteksi dan Analisis*
3. ***Tahap 3:*** *Penahanan (containment), Pemberantasan dan Pemulihan*
4. ***Tahap 4:*** *Aktivitas Pasca-Insiden*

Meskipun tahapan ini berurutan, pada kenyataannya dalam penanganan insiden digital prosesnya selalu berkesinambungan. Setiap proses ini juga perlu didokumentasikan dan diorganisir sehingga mampu untuk mengurangi kemungkinan insiden yang sama bisa terjadi kembali. Tentu, proses penanganan insiden pun perlu diadaptasi sesuai kebutuhan dan model kerja organisasi.

1. *Tahap 1: Persiapan*

Sebuah proses penanganan insiden dimulai ketika insiden terjadi. Penting untuk kita mencatat informasi-informasi dasar yang diperlukan terkait insiden. Pada tahap inilah, penyedia layanan perlu memastikan bahwa penerima layanan memang masuk dalam daftar dan kategori penerima layanan dan hal yang diminta atau dibutuhkan memang disediakan oleh penyedia layanan. Jika tidak masuk ke mandat layanan, maka kasus ditutup dan bisa direkomendasikan ke layanan lainnya.

Jika permintaan masuk dalam mandat penyedia layanan, maka perlu ada langkah vetting. Vetting adalah sebuah langkah mencari tahu lebih jauh soal permintaan yang datang. Setiap penyedia layanan perlu memiliki kebijakan vetting. Vetting adalah proses memastikan bahwa kita telah memverifikasi kebenaran dari sebuah permintaan yang masuk serta keaslian dari identitas dan aktivitas yang diklaim oleh pengadu. Memeriksa sebuah organisasi atau individu yang menghubungi kita adalah sebuah langkah keamanan bagi kita dan penguatan kepercayaan kita dalam jaringan.

Setelah memastikan mandat dan proses vetting selesai, kita perlu menyiapkan dokumentasi yang tepat.

2. *Tahap 2:* *Deteksi dan Analisis*

Meskipun idealnya proses penanganan insiden dimulai dari tahap persiapan, tetapi kenyataannya kerap kali proses dimulai dari tahap kedua, yakni deteksi dan analisis. Langkah pertama pada tahapan ini adalah deteksi yang bertujuan memastikan apakah yang pengadu alami memang benar-benar insiden keamanan. Penangan insiden perlu mengajukan sejumlah pertanyaan, seperti screenshot, pesan eror, atau hal-hal lain yang dianggap tidak wajar; hal-hal yang menunjukkan bahwa ini memang insiden keamanan. Penangan insiden harus terbuka terhadap banyak kemungkinan dan penuh pertimbangan terhadap indikator apa pun.

Perlu diingat, jika orang yang membutuhkan layanan kita sedang dalam keadaan stres, proses pengumpulan informasi penting bisa jadi sebuah proses viktimisasi ulang. Dalam kondisi seperti ini, baiknya data dikumpulkan dengan pertolongan orang lain yang dipercaya dan ditunjuk oleh penerima layanan.

Analisis adalah langkah selanjutnya untuk memahami apa yang sebenarnya terjadi dan sebabnya. Tentunya, semakin banyak bukti, semakin jelas pemahaman yang bisa diberikan oleh penyedia layanan. Proses analisis yang baik adalah proses yang dilakukan secara kolektif, bisa bersama-sama penangan insiden lainnya, sehingga kesalahan mengartikan fakta-fakta dan indikator bisa dihindari. Sebab kerap kali banyak korelasi antar-hal dalam sebuah insiden yang diartikan dengan salah dan terburu-buru.

Sebuah alat bantu online yang bisa digunakan untuk menganalisis berbagai jenis insiden keamanan digital yang sering terjadi adalah: https://digitalfirstaid.org/id/. Penangan insiden perlu mencatat segala informasi penting di setiap tahapan.

3. *Tahap 3:* *Penahanan (containment), Pemberantasan dan Pemulihan*

Setelah dipastikan bahwa memang yang diadukan adalah sebuah insiden keamanan digital, maka penangan insiden akan melakukan tahap tiga. Langkah pertama pada tahap ini adalah penanganan awal, layaknya "menghentikan pendarahan" pada insiden kecelakaan untuk memastikan bahwa penyerang (sumber insiden) tidak lagi punya akses lebih jauh pada aset-aset digital pengadu. Penangan insiden perlu dengan cepat memandu langkah penanganan ini untuk membatasi kerugian.

Langkah-langkah penanganan awal perlu dibuat dalam dokumentasi tertulis sehingga penangan insiden bisa mengaksesnya dengan cepat dan menggunakannya untuk kasus yang relevan. Dengan begitu, penangan insiden tidak perlu mengulang-ulang lagi kerja penyusunan panduan.

Langkah berikutnya, pembasmian, adalah menghapus apapun yang ditambahkan pada aset digital pengadu. Langkah ini tak selalu mudah karena aktor jahat biasanya sangat kreatif dalam merancang serangan.

Kemudian langkah pemulihan dilakukan untuk mengembalikan sistem atau pun aset digital yang terdampak dan melakukan tindakan untuk menghindari insiden baru. Maka, monitoring menjadi sangat penting untuk mendeteksi metode lain yang digunakan penyerang. Biasanya penangan insiden dalam kerja-kerja perubahan sosial dan masyarakat sipil tidak bisa memonitor langsung aset digital dari pengadu, maka langkah ini bisa dilakukan dengan memandu pengadu untuk memonitor mandiri.

Biasanya sebuah insiden keamanan digital tidak bisa diselesaikan oleh satu orang saja. Di sinilah pentingnya kerja tim yang baik dan berjejaring dengan penyedia layanan lainnya.



4. *Tahap 4:* *Aktivitas Pasca-Insiden*

Pada tahap akhir ini, penting bagi penangan insiden untuk mengumpulkan hasil observasi selama menangani insiden. Meskipun langkah-langkah mitigasi insiden tersebut sudah diketahui, bisa jadi ada cara-cara maupun pendekatan baru dalam penanganan insiden yang ditemukan dan perlu didokumentasikan.

Pencatatan *lesson learned* semacam ini akan meningkatkan kualitas dari penyedia layanan sehingga proses penanganan berikutnya bisa jadi lebih kreatif dan akurat. Sebaiknya, jangan menunda dokumentasi setelah penanganan insiden selesai sebab detail-detail kecil kerap mudah terlupakan.

Kadang-kadang, sebuah insiden juga terhubung dengan berbagai bentuk serangan lainnya kepada kelompok berbeda. Maka, peringatan perlu dilakukan. Hal ini bisa dilakukan dengan memberitahu jaringan, organisasi mitra, ataupun menyebarkan peringatan secara publik (jika memang ini dirasa tepat).



B. Langkah Penanganan: Doxxing

Doxxing kerap menjadi metode penyerang atau pihak lawan untuk menjatuhkan atau mengintimidasi sehingga kerap menimbulkan efek senyap *(chilling effect)* pada targetnya. Doxxing merupakan tindakan mempublikasikan informasi yang bisa mengidentifikasi seseorang secara pribadi atau mengungkap aspek kehidupan pribadi yang telah orang tersebut pilih untuk dirahasiakan, bukan publik. Doxxing sendiri berasal dari kata 'document' yang biasa kita singkat menjadi 'docs' dan diartikan secara teknis menjadi *merilis dokumen*. Dalam hal ini, maksudnya adalah dokumen yang berisi hal-hal pribadi dari seseorang. Formatnya bisa foto, video, dokumen, dan bentuk-bentuk lainnya.

Doxxing dapat berefek negatif pada kondisi psikososial dari target, keamanan pribadinya, relasi, bahkan sampai pekerjaan dan aktivitas yang sedang dilakukan. Belakangan doxxing tak hanya digunakan untuk mengintimidasi tokoh masyarakat, jurnalis, pembela HAM, dan aktivis, tetapi juga sering menargetkan orang-orang yang termasuk minoritas secara seksual atau kelompok yang terpinggirkan.

Pelaku doxxing mungkin telah memperoleh info pribadi dalam berbagai format atas seseorang dari berbagai sumber. Ini bisa termasuk membobol akun dan peranti pribadi. Namun, mungkin juga mereka mengungkap dan mengambil informasi yang dibagikan secara pribadi kepada teman, mitra, kenalan, atau rekan kerja. Dalam beberapa kasus, pelaku pelecehan dapat mengumpulkan informasi yang tersedia secara publik tentang seseorang dari media sosial atau catatan publik. Menyatukan informasi ini dengan cara-cara baru yang disalahartikan secara berbahaya juga bisa menjadi bagian dari doxxing.

Langkah penting disarankan dalam penanganan kasus doxxing, seperti pada kasus-kasus lainnya, adalah dokumentasi.

Dokumentasi dan Pendamping Kasus

Dokumentasi begitu penting untuk melakukan asesmen terhadap dampak dari insiden, mengidentifikasi asal serangan, dan mengembangkan respons yang dapat memulihkan keselamatan target doxxing. Mengerjakan dokumentasi bisa menimbulkan stres bagi yang terdampak bahkan yang menangani, maka pastikan target tidak mengalami trauma kembali saat menceritakan, susun strategi dengan bekerja dengan tim dan tunjuk pendamping korban yang dapat menjadi perwakilan dalam menceritakan kasus kembali.

Asesmen Kebutuhan Kasus

Pada tahap ini, setelah mengetahui garis besar dari insiden doxxing yang terjadi pada pengadu, penangan insiden bisa menganalisis: apakah ada risiko lainnya di luar digital, misalnya risiko fisik, psikososial, dan hukum

Jika dirasa ada risiko fisik dan hukum, maka kita perlu bekerja sama dengan lembaga lain yang menyediakan layanan perlindungan fisik dan hukum. Sementara pendampingan psikososial bisa dilakukan oleh penangan insiden yang berkapasitas di topik ini atau juga diarahkan ke lembaga yang berkapasitas.

Sementara untuk penanganan secara digital, pastikan terlebih dahulu di platform online manakah penyebaran informasi (doxxing) terjadi. Ini akan mempengaruhi bagaimana kita dapat membantu menanganinya.

Cek Informasi Apa Saja Yang Disebar

Informasi yang di-dox bisa berbagai macam tergantung apa yang pelaku dapatkan dan tujuannya menyerang. Biasanya informasi berupa:

- Informasi pribadi yang dapat mengidentifikasi target, seperti alamat, nomor, telepon, NIK, rekening bank, dll;
- Media pribadi yang tidak disetujui untuk disebar, termasuk konten intim (gambar, video, audio, teks);
- Nama alias atau samaran yang digunakan untuk ekspresi atau kerja di isu tertentu.
- Menghapus Doxxing dari Tampilan Publik

Pastikan sebelum dihapus, serangan dan bukti doxxing sudah didokumentasikan dengan baik. Hal ini penting agar kita bisa membantu secara teknis dengan lebih jitu, terlebih lagi jika kasus ingin dibawa ke ranah hukum. Lagi-lagi, jangan lupa juga perhatikan kondisi psikologis target yang mengalami doxxing, jika dirasa target sedang mengalami stres setelah kena serang, baiknya minta orang lain yang dipercaya untuk mendokumentasikannya sehingga tidak terjadi trauma ulang.

Karena membutuhkan platform publik untuk bekerja, maka kasus doxxing akan bergantung pada di mana si penyerang membagikan informasi soal seseorang. Platform online mana yang menjadi lokasi penyebaran doxxing akan mempengaruhi bagaimana kita bisa bertindak.

- **Jika doxxing disebar di platform online atau media sosial** yang basisnya di negara-negara dengan hukum yang mengikat tanggung jawab perusahaan terhadap pengguna layanan (seperti Uni Eropa), moderator dari platform akan bersedia untuk membantu kasus doxxing. Cari tahu dulu basis negara dari platform online yang digunakan untuk penyebaran doxxing tersebut.

- **Kadang doxxing juga disebar di situs-situs kecil yang tidak populer**, lalu link ke situs tersebut disebarkan di media sosial. Biasanya situs-situs tersebut di-host di negara yang tidak punya perlindungan hukum atas data dengan baik. Dalam hal ini akan sulit untuk menghubungi pemilik situs atau mencari tahu siapa yang menjalankannya. Namun, jika link di media sosial yang lebih bertanggung jawab bisa membantu menghapusnya,

setidaknya dapat mengurangi banyaknya orang yang dapat melihat informasi doxxing.

• **Menutup Akun Sementara**
Jika target doxxing memiliki nama samaran atau alias yang digunakan khusus untuk mengekspresikan diri atau mengerjakan isu-isu tertentu, kemudian dalam serangan doxxing nama-nama alias tersebut dikaitkan dengan identitas asli dari target, maka kita bisa menyarankan untuk menutup akun dengan nama tersebut untuk sementara. Tentu jika ini adalah cara yang mungkin bagi target serangan.

• **Jika bisa menutup akun**
Jangan lupa beritahu terlebih dahulu risiko menutup akun, seperti kehilangan akses ke layanan dan data, juga kontak dan rekan online. Sarankan langkah mitigasi sebelum menutup akun, seperti melakukan back up data penting, memberitahu kontak dekat terlebih dahulu, dan seterusnya tergantung kebutuhan target terhadap akunnya.

• **Jika tetap perlu dan ingin menggunakan akun**
Lakukan peninjauan terhadap praktik keamanan informasi pribadi, seperti meningkatkan keamanan akun (ganti password, perkuat 2FA, meningkatkan pengaturan privasi).

• **Jika Doxxing Berisi Media Intim**
Gunakan Aturan Hak Cipta
Kita bisa menggunakan aturan hak cipta jika media yang disebar dalam doxxing secara properti intelektual adalah milik kita.

Gunakan tautan ini untuk mengirim permintaan penghapusan karena pelanggaran hak cipta ke platform jejaring sosial utama:

1. ***Facebook***
2. ***Instagram***
3. ***TikTok***
4. ***Twitter***
5. ***Youtube***

Pahami Aturan yang Berlaku
Jika target ingin memproses ke kalur hukum, cek cara melaporkan pelanggaran aturan privasi atau berbagi media intim/konten secara hukum silakan lihat sumber berikut.

Petakan Kebutuhan Psikologis Target
Dalam kasus penyebaran konten intim nonkonsensual, dampak psikologis pada target sulit terelakkan. Maka, penangan insiden perlu lebih sensitif dan mempertimbangkan aspek psikososial. Cari dukungan psikososial yang tepat jika kita tidak memiliki kapasitas terkait ini. *(Lihat bagian Psikososial)*

• **Penguatan Keamanan Digital**

• **Jika doxxing berisi informasi atau dokumen yang aksesnya hanya dimiliki target atau beberapa orang yang dipercaya**, mungkin bisa dianalisis bagaimana pelaku bisa mendapatkan

informasi tersebut. Cek lagi keamanan data pribadi target, termasuk peranti (ponsel, komputer) dan akun.

• **Nyalakan Peringatan Google** untuk cek apakah nama atau nama samaran yang terkait doxxing kembali muncul dengan materi doxxing yang sama.

C. Langkah Penanganan: Akun Diambil Alih

Akun merupakan salah satu identitas digital yang mendasar bagi aktivitas kita, termasuk untuk komunikasi dan kerja-kerja masyarakat sipil. Kolaborasi, berbagi, dan advokasi pergerakan jadi lebih leluasa dan mudah, tapi dengan konsekuensi mudah pula menjadi sasaran empuk oknum yang berniat jahat.

Serangan terhadap akun bisa melalui beragam cara. Mulai dari phishing yang bertujuan mencuri kredensial akun sampai pelaporan massal terhadap akun yang mengakibatkan akun diblokir. Berikut ini panduan jika anda kehilangan akses ke salah satu akun anda beserta langkah pengamanan preventifnya.

• **Jika Akun Dinonaktifkan/Blokir**
Terkadang Anda tidak dapat masuk ke akun karena telah diblokir atau dinonaktifkan oleh platform mungkin karena terjadi pelanggaran Persyaratan Layanan atau peraturan platform. Hal ini dapat terjadi saat akun Anda dilaporkan secara masif, atau saat mekanisme pelaporan dan dukungan platform disalahgunakan dengan tujuan untuk menyensor konten daring.

Jika Anda melihat pesan bahwa akun Anda dikunci, dibatasi, dinonaktifkan atau ditangguhkan, dan Anda yakin ini adalah kesalahan. Ikuti mekanisme pengajuan banding apa pun yang disertakan dengan pesan tersebut. Anda dapat menemukan informasi tentang cara mengajukan banding di tautan berikut:

1. *Facebook*
2. *Instagram*
3. *Twitter*
4. *Youtube*

- **Jika Ada yang Mengambil Alih Akun**

// Cek akses akun

Akun email dan media sosial umumnya memiliki pengaturan untuk memonitor perangkat mana saja yang mengakses akun kita. Melalui pengaturan ini, kita bisa mengetahui jika ada perangkat asing yang terhubung ke akun kita. Jika ini terjadi, segera dokumentasikan terlebih dahulu keterangan perangkat dan waktu perangkat terhubung (log in) ke akun kita, kemudian hapus perangkat tersebut dari akun kita.

Jika hal ini terjadi, artinya kredensial akun kita sudah tidak lagi aman, maka sangat disarankan untuk mengubah kata sandi akun tersebut, pastikan kata sandinya kuat. Jika belum, aktifkan 2FA pada akun tersebut. Untuk moda 2FA yang lebih kuat, gunakan aplikasi otentikator.

// Asesmen kembali

Pastikan akun yang terambil alih tersebut terhubung ke layanan online apa saja. Misalnya saja kita menggunakan email yang terambil alih untuk log in ke media sosial dan layanan e-commerce, maka ubah dahulu kata sandi dari akun-akun tersebut. Bahkan jika ingin lebih aman lagi, ubah juga email registrasinya dengan email lain yang tidak terambil alih.

- Mengelola identitas digital (akun)

- Apakah kita mencampur penggunaan akun atau identitas digital?

- Sejauh apa personal akun kita terhubung dengan akun kerja kita?

- Apakah ada aktivitas online yang berisiko jika kita menggunakan akun personal/asli kita?

- Tips tambahan keamanan akun

Silakan baca rekomendasi kami berikut ini untuk membantu meminimalkan kemungkinan kehilangan akses ke akun Anda di masa mendatang.

- Sangat disarankan untuk mengaktifkan autentikasi 2 langkah (2FA) untuk semua akun Anda di semua platform yang mendukungnya.

- Jangan pernah menggunakan kata sandi yang sama untuk lebih dari satu akun. Jika Anda masih melakukannya, Anda sebaiknya mengubahnya dengan kata sandi unik untuk setiap akun Anda.

- Menggunakan pengelola kata sandi dapat membantu Anda membuat dan mengingat kata sandi yang unik dan kuat untuk semua akun Anda.

• Waspadalah saat menggunakan jaringan Wi-Fi publik terbuka yang tidak tepercaya, dan sebisa mungkin gunakan VPN atau Tor saat terhubung dengan jaringan tersebut.

D. Langkah Penanganan: Peranti Mobile

Salah satu insiden yang umum terjadi pada peranti digital adalah malware. Malware (malicious software = software yang merugikan) telah berkembang dan meningkat dalam tingkat kecanggihannya seiring waktu berjalan. Ancaman-ancaman yang ditimbulkan oleh serangan ini sangat beragam dan dapat berdampak serius pada infrastruktur serta data pribadi maupun organisasi. Malware dapat muncul dalam berbagai bentuk seperti virus, phishing, ransomware, trojan, dan rootkit. Contoh ancaman tersebut antara lain meliputi kerusakan pada peranti, pencurian data sensitif seperti informasi keuangan atau login rekening bank, pemerasan untuk membayar tebusan dengan mengambil alih perangkat.

Melalui panduan bagian ini, kita akan mempelajari hal-hal dasar yang dapat kita lakukan secara mandiri jika kita merasa peranti kita bermasalah. Dengan mengetahui langkah-langkah dasar, harapannya kita dapat mengurangi rasa panik jika insiden terjadi. Selain itu, sejumlah langkah preventif dasar juga dijelaskan pada bagian akhir.

// Gejala-gejalanya

Gejala yang umum dianggap sebagai mencurigakan tapi tidak cukup jadi alasan

- Bunyi klik saat panggilan telepon
- Baterai terkuras tak terduga
- Suhu terlalu panas saat tak digunakan
- Peranti beroperasi dengan lambat

Gejala yang umum dianggap sebagai mencurigakan tapi tidak cukup jadi alasan

- Peranti kerap kali memulai ulang (restart) dengan sendirinya
- Aplikasi crash, terutama setelah melakukan suatu tindakan
- Pembaruan sistem operasi dan/atau patch keamanan gagal berulang kali
- Lampu indikator aktivitas webcam menyala saat sedang tidak digunakan
- Kemunculan berulang kali "Blue Screens of Death" atau kernel panic
- Window yang berkedip
- Peringatan antivirus

// Asesmen Situasi

1. Mendapatkan surel atau postingan di media sosial yang mengajak untuk membuka lampiran atau mengeklik tautan.
2. Ajakan untuk mengunduh atau memasang perangkat lunak dari sumber yang tidak terpercaya.
3. Ajakan untuk memasukkan nama pengguna dan kata sandi ke situs web yang dibuat sedemikian rupa agar terlihat tepercaya.
4. Diam-diam terpasang aplikasi perangkat pengintai (spyware) komersial di peranti saat tanpa pengawasan dan tidak terkunci.

// Langkah Mitigasi

1. Backup segera.

2.	Pastikan akun apa saja yang terlogin di perangkat tersebut.
3.	Ubah password dari akun-akun terpenting, jika memungkinkan, semuanya yang terlogin di perangkat.
4.	Jika ada 2FA dan belum diaktifkan, segera aktifkan 2FA pada akun-akun tersebut. Jika mau lebih kuat, pakai security key sebagai metode 2FA.
5.	Cek siapa saja yang punya akses ke akun terdaftar di HP (Gmail atau Apple).
6.	Beri tahu teman satu tim atau yang dipercaya (tergantung level insidennya).

// Langkah analisis (forensik dasar)

ANDROID	iPHONE
Cek aplikasi yang terinstal.	Review akun iCloud.
Cek penyimpanan.	Cek aplikasi terinstal.
Cek apakah ponsel sudah di-root.	Cek apakah ponsel sudah di-jailbreak.
Cek apakah pilihan developer (developer options) aktif.	Cek Mobile Device Management Profiles.
Cek apakah Install Unknown Apps diaktifkan pada pengaturan.	Analisis aplikasi Exodus dan file/url dengan VirusTotal.
Analisis aplikasi Exodus dan file/url dengan VirusTotal.	

// Langkah Lanjutan

1.	Menggunakan tools forensik digital. Di antaranya: MVT tools, Androidqf, PiRogue.
2.	Bekerja sama dengan penyedia layanan yang dapat melakukan forensik digital.

// Preventif

Meminimalisir dampak jika insiden terjadi.

1.	Pastikan perangkat dienkripsi.
2.	Autolock layar (terkunci otomatis saat tidak aktif).
3.	Tahu kapan log out layanan-layanan pada perangkat.
4.	Selalu back up.
5.	Manajemen data dan identitas.
6.	Update dan upgrade.

Sumber:
- *Tech Care, https://tech-care.cc/*
- *Digital First Aid Kit, https://digitalfirstaid.org/id/*
- *Security Without Borders, https://github.com/securitywithoutborders*

KEAMANAN FISIK



03

A. Kesadaran Situasional

Memahami perubahan di sekitar Anda merupakan bekal penting bagi setiap orang, tidak terlepas pembela HAM dan jurnalis. Kemampuan mengadaptasi dan mengeksekusi pilihan jadi modal utama untuk mengambil keputusan saat bekerja di lingkungan yang cukup kompleks.

Berbekal pengetahuan sebelumnya, Anda secara menerus mengambil informasi dari lingkungan sekitar guna membentuk gambaran umum agar dapat membantu persepsi Anda dalam proses pengambilan keputusan di masa depan.

Karena situasi di sekitar Anda sangat dinamis, penting kiranya Anda tetap fleksibel, terus mengamati, menafsirkan kondisi lingkungan. Tujuannya, hanya satu, membantu Anda mengambil keputusan terbaik.

// Prinsip 4 A

A = Ases situasi Anda
Contohnya, Anda mengetahui apa yang ada di hadapan Anda.

A = Analisa informasinya
Anda mengidentifikasi informasi apa yang penting dan memerlukan prioritas.

A = Artikulasi
Berdasarkan analisa Anda, apakah Anda perlu telepon orang, membuat catatan, atau melapor via email kepada pihak lain? Ini momen untuk anda mempertimbangkan beragam pilihan yang ada.

A = Aksi
Buat keputusan berdasarkan 3A tadi lalu ambil tindakan.

// Kode Warna

Saat Anda melakukan pekerjaan atau tugas terkait dengan kesadaran situasional, sebaiknya mengingat kondisi dengan kode warna Cooper seperti di bawah ini:



Putih
Tidak ada persiapan dan tidak mampu mengambil tindakan.



Kuning
Bersiap, waspada, tidak tegang. Kesadaran situasional baik.



Orange
Waspada terhadap kemungkinan bahaya. Siap beraksi.



Merah
Siap bertindak. Fokus pada kedaruratan yang dihadapi.



Hitam
Panik. Fisik lemah dan mental jatuh.

Penerapan kode warna ini diadaptasi dari Jeff Cooper yang menulis buku "Prinsip Pertahanan Diri" atau "Principles of Personal Defense". Kode warna ini diajarkan pada petugas kepolisian terkait peningkatan kesiapan saat menggunakan kekuatannya.

Penerapan kode warna ini adalah proses mental bukan proses fisik. Anda bisa saja berada dalam kondisi 'Putih' jika sedang tidur. Namun, sebagai pembela

HAM atau jurnalis yang turun ke lapangan saat mendampingi atau meliput aksi massa, kondisi 'Putih' akan sangat tidak menguntungkan Anda.

Kondisi Kuning

Kondisi 'Kuning', Anda tetap santai, tetapi sadar akan siapa dan apa yang ada di sekitar Anda. Ini berarti Anda memantau pemandangan, suara, beragam kondisi di sekitar. Apakah ada yang tidak biasa atau semuanya normal-normal saja.

Kondisi 'Kuning' tidak bisa disamakan dengan ketakutan irasional terhadap orang atau tempat. Anda hanya memindahkan tingkat kewaspadaan Anda ke tingkat perhatian yang bakal mencegah Anda terkejut dengan tindakan orang lain.

Misalnya, saat memilih tempat duduk di restoran, posisikan diri Anda untuk melihat pintu masuk atau untuk mencari lokasi duduk dengan tanpa atau sangat sedikit orang di belakang Anda.

Jika Anda diserang dalam kondisi 'Kuning', seharusnya tidak mengejutkan. Respon Anda terhadap ancaman seharusnya sudah direncanakan sampai batas tertentu.

Kondisi Orange

Dalam kondisi 'Oranye', Anda telah mengidentifikasi sesuatu yang menarik yang mungkin atau mungkin tidak terbukti menjadi ancaman. Dalam kondisi ini, 'radar' Anda dipersempit untuk berkonsentrasi pada kemungkinan ancaman dan akan tetap begitu hingga Anda merasa puas karena tidak ada ancaman.

Misalnya, Anda mendapati sesuatu yang terlihat tidak semestinya atau tidak pada tempatnya seperti kondisi normal, maka kesadaran Anda berubah dari kesadaran umum menjadi lebih fokus ke arah tertentu. Sama halnya dengan perangai peserta aksi yang tadinya tenang menjadi lebih agresif, maka fokus Anda adalah mengantisipasi kemarahan peserta aksi.

Kondisi Merah

Jika fokus perhatian Anda dalam kondisi 'Oranye' melakukan sesuatu yang Anda temukan mengancam, maka Anda beralih ke kondisi 'Merah'.

Pada kondisi 'Merah' Anda tidak akan terkejut ketika mendapatkan aksi dari sesuatu yang Anda sudah tandai sebagai ancaman.

Misalnya, saat ada peserta aksi demonstrasi yang hendak menyerang atau berlari ke arah Anda, maka Anda akan memilih bergeser ke lokasi yang memungkinkan Anda melarikan diri atau malah memilih membela diri seandainya Anda terlatih.

Kondisi Hitam

Analisa situasional dapat membantu menentukan kondisi dan persiapan Anda. Jangan sampai kondisi diri berada di warna Putih atau Hitam. Kedua kondisi ini sama sekali tidak akan membantu Anda atau tim dalam mengantisipasi kondisi yang dinamis di lapangan.

Kondisi 'Hitam' terjadi saat Anda malah panik dan tidak bisa mengambil keputusan dalam sebuah kondisi yang mungkin berbahaya bagi Anda.

5

Cara Meningkatkan Kesadaran Situasional Anda

1. Menilai risiko dari semua 'sudut'

• Belajar memerhatikan segala sesuatu dengan fokus '360 derajat'--bukan fokus Anda sendiri

• Pertimbangkan seberapa besar kemungkinan adanya faktor-faktor lain yang memengaruhi situasi yang Anda tidak sadari.

• Bertanya tanpa menghakimi adalah faktor kunci keberhasilan kesadaran situasional.

---

2. Pertimbangkan alam bawah sadar

• Kita memiliki beberapa bias kognitif. Implikasinya perlu diperhitungkan dalam kesadaran situasional kita.

• Dalam rangka merespon kesadaran situasional, buat keputusan yang logis, dan memerhatikan fokus strategi untuk masa depan, alam bawah sadar harus dilibatkan dan dinilai.

• Jangan biarkan bias yang tidak disadari memengaruhi pandangan Anda dan berpotensi menimbulkan risiko pada tim dan percayai nalurimu!

3. Selalu berkomunikasi

• Mengomunikasikan persepsi atas risiko adalah bagian penting dari strategi kesadaran secara utuh. Setiap strategi yang efektif memerlukan semua orang terlibat dan jalan terbaik meraihnya adalah mengomunikasikan setiap tahap penilaian risiko atau potensi bahaya pada semua yang terlibat.

• Dalam praktiknya, bisa beritahu seseorang soal bahaya yang Anda lihat, atau tentang risiko yang Anda anggap akan datang. Ini juga bisa berarti meminta bantuan untuk situasi atau tugas kata pelatihan kesadaran situasional Anda mengidentifikasi ini berisiko jika dilakukan satu orang saja.

• Bagi pemimpin, hal ini bisa berarti menerapkan praktik dan protokol yang tepat saat berkomunikasi dengan tim jika/ketika situasi berubah.

4. Buat kesadaran situasional sebagai bagian dari proses orientasi Anda dan tawarkan pelatihan berkelanjutan

• Beritahu semua kolega baru terkait kebijakan dan proses strategi Anda. Terapkan beberapa pelatihan situasional sebagai bagian dari proses orientasi juga atau sebagai bagian dari pelatihan berkelanjutan. Sesi pelatihan harus mencakup skenario realistis yang disesuaikan dengan bidang Anda

.

• Dengan begitu, Anda membantu menumbuhkan budaya manajemen yang sehat dan aman dan memungkinan semua anggota tim merasa nyaman menilai dan melaporkan risiko apa pun.

• Anda dapat membumikan tahapannya atau penugasan dan tambahkan skenario 'bagaimana-jika' pada mereka.

5. Latih kesadaran situasional

• Ini harus jadi upaya dari semua pihak guna memiliki pandangan 360 derajat terhadap situasi dan kondisi. Tunjukkan kepada orang lain betapa pentingnya hal ini. Dibutuhkan latihan untuk menghindari gangguan dan membiasakan diri menggunakan penglihatan tepi anda.

• Kemampuan memanfaatkan penglihatan samping ini memberikan kemampuan melihat objek dan gerakan di luar garis pandang langsung. Ini membutuhkan latihan.

*Saat Anda menghadapi kondisi yang tidak biasa dan memerlukan pengambilan keputusan, ada baiknya menerapkan langkah seperti yang ada pada **S.A.F.E.R Model.***

Model ini membantu Anda mengevaluasi potensi situasi sulit, kontrol dan pilih respon terbaik

STEP BACK

Jangan terburu-buru, termasuk saat Anda hendak menolong seseorang

Tahan tindakan Anda agar bisa mengevaluasi apa yang sebenarnya terjadi

Mundur secara mental dan emosional, kedepankan rasionalitas soal apa yang terjadi dan apa respon yang terbaik

ASSESS

Identifikasi potensi bahaya dengan prinsip OOT (Orang, Objek, Tempat)

Identifikasi juga perasaan, kekuatan dan kelemahan Anda

FIND HELP

Pertimbangkan bantuan apa yang Anda perlukan

Layanan darurat

Rekan kerja

Pendamping

Pengambil keputusan/manajer

Mencari pertolongan dapat membantu kita untuk mengatasi dan berurusan dengan insiden secara rasional. Skala pertolongan yang diperlukan tergantung dari isu, situasi, dan perilaku semua yang terkait

EVALUATE OPTIONS

Tiga pilihan utama:

Keluar ke tempat aman

Alihkan kontrol ke orang lain

Hadapi langsung orang yang dimaksud

RESPONSE

Respon secara tepat
Evaluasi terus menerus:

Ancaman

Efektifitas dari strategi

Kemampuan anda untuk berpikir dan berperilaku rasional

B. Pendekatan Bertahap untuk Mengelola Risiko

// Manajemen Risiko

Manajemen risiko adalah proses proaktif yang membantu Anda mengidentifikasi dan mengurangi risiko dan bahaya yang terkait dengan skenario atau lingkungan tertentu.

Upaya ini harus direncanakan, sistematis, dan mencakup semua bahaya yang dapat diperkirakan secara wajar dan risiko terkait. Sebelum kita melanjutkan, mari kita perjelas apa yang kita maksud dengan istilah bahaya dan risiko.

"Bahaya" - suatu situasi atau hal yang berpotensi merugikan seseorang

"Risiko" - situasi yang melibatkan paparan pada bahaya

Setelah mengidentifikasi arti istilah-istilah ini, mari kita lihat bagaimana kita mengidentifikasi dan mengelolanya.

// Mengidentifikasi Risiko

Sebelum kita dapat melihat langkah-langkah untuk mengelola risiko, pertama-tama kita perlu mengidentifikasi ancaman dan bahaya dari setiap tahap tugas atau penugasan. Kita telah membahas proses membagi ini menjadi

KEMUNGKINAN	***KONSEKUENSI***	
	1. TIDAK SIGNIFIKAN	***2. MINOR*** (Perlu P3K)
1. LANGKAH	***Rendah***	***Rendah***
2. JARANG	***Rendah***	***Rendah***
3. POTENSIAL	***Rendah***	***Sedang***
4. SERING	***Sedang***	***Sedang***
5. HAMPIR PASTI	***Sedang***	***Tinggi***

beberapa langkah, meneliti setiap langkah, serta melihat "bagaimana seandainya". Ini adalah tahap pertama dalam penilaian risiko.

Setelah kita mengidentifikasi perlakuan dan bahaya, yang juga dikenal sebagai "risiko", kita selanjutnya dapat melihat cara kita dapat mengelola risiko ini.

3. SEDANG (Perlu bantuan medis dan berhenti kerja)	***4. MAJOR*** (Sakit berkepanjangan atau luka serius)	***5. BENCANA*** (Kematian atau lumpuh atau sakit permanen)
Sedang	***Sedang***	***Sedang***
Sedang	***Sedang***	***Tinggi***
Tinggi	***Tinggi***	***Ekstrim***
Tinggi	***Tinggi***	***Ekstrim***
Tinggi	***Ekstrim***	***Ekstrim***

// Mengelola Risiko

Ada empat opsi utama ("tindakan pengendalian") yang kita miliki saat mengelola risiko:

- ***Menghindari***
- ***Menghilangkan***
- ***Mengurangi***
- ***Memindahkan***

Menghindari risiko; Satu contohnya adalah; jika selama penelitian dan perencanaan Anda mengidentifikasi area yang sangat berbahaya di sepanjang rute yang Anda pertimbangkan untuk diambil dalam tugas Anda, maka hanya dengan memutuskan untuk mengambil rute lain saja, Anda dapat menghindari bahaya itu sepenuhnya. Dalam hal ini Anda mungkin telah menghindari sepenuhnya risiko itu.

Membatasi risikonya; contohnya adalah; saat melakukan penelitian Anda ke lokasi dan tugas, Anda menyadari bahwa tempat itu berada di area yang sangat berbahaya, dan memutuskan risiko meliput itu jauh lebih besar daripada nilai liputannya, dan karena itu memutuskan untuk tidak melanjutkan tugas. Maka dengan demikian telah menghilangkan risiko itu sepenuhnya.

Mengurangi risikonya.

- Melakukan pelatihan yang sesuai sehingga Anda dapat menghadapi kemungkinan keadaan darurat yaitu pelatihan medis sebelum meliput zona perang, protes, atau bencana alam
- Memahami kondisi lapangan dan telah memutuskan area dan/atau posisi paling aman untuk melaksanakan tugas
- Memiliki tingkat peralatan alat pelindung diri yang sesuai, dan mengetahui cara memasang dan memakainya dengan benar
- Bekerja sama dengan orang lain sehingga Anda dapat saling menjaga
- Memiliki kontak darurat dan Prosedur "melapor"

Kunci dari mengurangi risiko adalah dengan memiliki pendekatan "berlapis" demi keselamatan dan keamanan Anda. Yang sederhananya adalah memiliki tindakan "cadangan" jika terjadi kesalahan. Memindahkan risiko berarti Anda mengalihkannya ke orang lain. Contohnya adalah mengasuransikan peralatan atau asuransi perjalanan Anda. Jadi tanggung jawab dipegang perusahaan asuransi yang kemudian harus menanggung biaya barang atau situasi apa pun yang ditanggung asuransi mereka.

// Empat Langkah Mengelola Risiko

Langkah 1 - Cara mengenali bahaya

Mengenali bahaya melibatkan identifikasi penyebab dan situasi yang berpotensi membahayakan orang. Bahaya umumnya muncul dari aspek pekerjaan berikut dan interaksinya:

- Lingkungan kerja fisik
- Peralatan, material, dan bahan yang digunakan
- Tugas kerja dan cara pelaksanaannya, dan
- Perencanaan dan manajemen kerja.

Langkah 2 - Nilai risikonya

Jika perlu – pahami sifat bahaya yang dapat ditimbulkan oleh bahaya, seberapa serius bahaya tersebut dan kemungkinan terjadinya. Langkah ini mungkin tidak diperlukan jika Anda menghadapi risiko yang diketahui, dengan kontrol yang diketahui. Sebuah penilaian risiko melibatkan pertimbangan apa yang bisa terjadi jika seseorang terkena bahaya dan kemungkinan hal itu terjadi dengan menentukan:

- Seberapa parah risikonya?
- Apakah tindakan pengendalian yang ada efektif
- Tindakan apa yang harus Anda ambil untuk mengendalikan risiko, dan
- Seberapa mendesak tindakan yang perlu diambil.

Banyak bahaya dan risiko terkaitnya telah diketahui dengan baik dan telah ditetapkan dengan baik serta langkah-langkah pengendalian yang dapat diterima. Dalam situasi ini, langkah kedua untuk menilai risiko secara formal tidak diperlukan. Jika setelah mengidentifikasi bahaya Anda sudah mengetahui risikonya dan cara mengendalikannya secara efektif, Anda cukup menerapkan kontrol tersebut.

Penilaian risiko dapat dilakukan dengan berbagai tingkat detail bergantung pada jenis bahaya dan informasi, data, dan sumber daya yang Anda miliki. Ini bisa hanya dengan berdiskusi dengan pekerja atau melibatkan alat dan teknik analisis risiko khusus yang dikembangkan untuk risiko tertentu atau direkomendasikan oleh profesional keselamatan. Pada beberapa situasi yang kompleks, saran ahli atau spesialis mungkin berguna saat melakukan penilaian risiko.

Kapan penilaian risiko harus dilakukan?

Penilaian risiko harus dilakukan ketika:

- Terdapat ketidakpastian tentang cara bahaya dapat mengakibatkan cedera atau penyakit
- Aktivitas kerja melibatkan sejumlah bahaya yang berbeda

Mencari tahu bagaimana risiko bahaya dapat mengakibatkan bahaya

Dalam kebanyakan kasus, insiden terjadi sebagai akibat dari rantai peristiwa dan kegagalan satu atau beberapa mata rantai dalam rantai itu. Jika satu atau lebih peristiwa dapat dihentikan atau diubah, risiko dapat dihilangkan/dikurangi.

Cara yang paling efektif adalah dengan membagi tugas atau penugasan menjadi beberapa langkah, melihat setiap langkah dan mempertimbangkan pertanyaan "bagaimana seandainya? Jadi, memikirkan semua kemungkinan yang bisa terjadi.

Dalam memikirkan bagaimana setiap risiko bahaya dapat menimbulkan bahaya, Anda harus mempertimbangkan:

- Efektivitas tindakan pengendalian yang ada dan apakah tindakan tersebut mengendalikan semua jenis bahaya
- Bagaimana pekerjaan sebenarnya dilakukan, daripada mengandalkan manual dan prosedur tertulis, dan
- Situasi yang jarang atau tidak

normal, serta bagaimana biasanya hal-hal semestinya terjadi.
- Mengetahui seberapa parah suatu bahaya dapat terjadi

Mengetahui kemungkinan terjadinya bahaya

Kemungkinan seseorang terkena bahaya dapat diperkirakan dengan mempertimbangkan hal-hal berikut:

Seberapa sering tugas itu dilakukan? Apakah ini membuat bahaya lebih mungkin atau kurang mungkin terjadi? Seberapa seringkah orang berada di dekat risiko bahaya? Seberapa dekatkah orang dengan risiko bahaya itu? Apakah pernah terjadi sebelumnya, baik di tempat kerja maupun di tempat lain? Seberapa seringkah?

Anda dapat menilai kemungkinan sebagai salah satu dari berikut ini:

- Pasti terjadi - diharapkan terjadi di sebagian besar situasi
- Sangat mungkin - mungkin akan terjadi di sebagian besar situasi
- Mungkin - mungkin terjadi sesekali
- Tidak mungkin - suatu saat bisa terjadi
- Langka - hanya dapat terjadi dalam keadaan luar biasa.

Langkah 3 - Mengontrol risiko

Menerapkan langkah-langkah pengendalian yang paling efektif yang cukup praktis dalam situasi dan memastikan bahwa langkah-langkah itu tetap berjalan dari waktu ke waktu.

Langkah 3 - Mengontrol risiko

Menerapkan langkah-langkah pengendalian yang paling efektif yang cukup praktis dalam situasi dan memastikan bahwa langkah-langkah itu tetap berjalan dari waktu ke waktu.

Langkah 4 - Meninjau tindakan pengendalian

Pantau untuk menentukan apakah tindakan tersebut efektif dan berdampak positif dalam menghilangkan atau meminimalkan risiko. Jika masalah ditemukan, kembalilah ke langkah-langkah manajemen risiko, tinjau informasi Anda, dan buat keputusan lebih lanjut tentang tindakan pengendalian.

C. Keamanan Tempat Kerja

Apa Itu Keamanan Kantor/tempat Kerja

Dalam arti sebenarnya, kantor/tempat kerja berarti tempat terkoordinasinya kegiatan-kegiatan suatu organisasi. Kantor bisa sebagai pusat kegiatan administrasi dan pusat komunikasi

Selanjutnya, keamanan kantor/tempat kerja mengacu pada langkah-langkah yang diambil untuk melindungi orang (termasuk tamu/pengunjung), aset, dan informasi dari ancaman fisik dan digital. Ancaman ini bisa datang dalam berbagai bentuk, mulai dari pencurian, kekerasan, dan vandalisme, hingga risiko keamanan digital seperti serangan siber, pembobolan data, dan peretasan. Saat mempertim-bangkan keamanan di kantor/tempat kerja, penting untuk mengambil tindakan yang tepat untuk mencegah kedua hal

tersebut, ancaman keamanan fisik dan digital. Keamanan fisik mengacu pada semua aset fisik di kantor/tempat kerja, seperti karyawan, peralatan, pengunjung, dan kantor suatu organisasi. Di sisi lain, keamanan digital mengacu pada perlindungan data, informasi, ide, dan sistem. Mungkin kita tidak dapat melihat atau menyentuh aset-aset ini, namun aset-aset ini penting bagi kesuksesan dan integritas bisnis suatu organisasi.

Pentingnya Tempat Keamanan Kantor/ Kerja

Keamanan di tempat kerja menjaga karyawan dan kantor fisik Anda aman dari bahaya dan risiko . Strategi keamanan tempat kerja harus melindungi data dan informasi penting organisasi dari peretas dan ancaman keamanan siber lainnya. Hal ini juga membuat organisasi tetap mematuhi undang-undang dan peraturan terbaru di negara atau wilayah suatu organisasi berada. Di tempat kerja modern saat ini, ada banyak hal yang harus dilindungi. Dan tidak semuanya terlihat oleh mata atau mudah dikenali.

Untuk menjaga keselamatan dan keamanan semua orang dan segala sesuatu di tempat kerja, organisasi perlu menggunakan teknologi, kebijakan, dan pelatihan yang sesuai.

Praktek Terbaik Keamanan Tempat Kerja

1. Sistem Manajemen Pengunjung

Meja resepsionis merupakan barisan pertahanan pertama suatu kantor. Terapkanlah sistem manajemen pengunjung yang membantu resepsionis dalam melakukan proses keamanan dengan ramah. Sistem ini akan menyaring pengunjung, melakukan pemeriksaan lintas referensi dengan daftar hitam, dan memberikan peringatan kepada pihak yang berwenang jika ada kegiatan yang mencurigakan. Semua ini dilakukan secara otomatis dan tidak mencolok. Selain itu, aplikasi ini akan mencatat kedatangan dan keberangkatan setiap pengunjung, memberikan Anda pemahaman tentang siapa yang berada di lokasi, kapan, dan seberapa sering.

2. Kontrol Akses

Kontrol akses adalah metode fisik yang mengatur atau membatasi akses ke suatu ruangan. Ini memastikan bahwa setiap orang yang memasuki ruangan dimaksudkan untuk berada di sana. Kontrol akses dapat berupa aplikasi ponsel, pengenalan wajah, atau kode masuk. Mengatur kontrol akses adalah cara pasti untuk mencegah orang yang tidak diinginkan masuk ke area Anda.

3. Kamera Pengawas

Meskipun tempat kerja suatu organisasi mungkin tidak sering menjadi tempat kejahatan, memasang kamera pengawas tetaplah penting. Kamera ini membantu mencegah kejahatan dan memberikan bukti jika terjadi pelanggaran keamanan. Ini adalah alat yang efektif untuk melacak aktivitas di tempat kerja.

4. Rencana Darurat dan Evakuasi

Organisasi perlu memiliki rencana untuk menghadapi situasi darurat, baik itu bencana alam maupun ancaman eksternal seperti penyusup. Perlu penyusunan rencana dengan langkah-langkah evakuasi dan informasi kontak darurat.

TIPS TAMBAHAN:

Dengan penjadwalan karyawan, organisasi dapat melacak secara tepat berapa banyak karyawan yang berada di lokasi. Informasi ini, bersama dengan data check-in pengunjung, dapat membantu Anda memahami berapa banyak orang yang perlu dievakuasi dari gedung pada situasi darurat (gempa bumi, kebakaran, amuk massa di depan kantor). Dengan integrasi yang baik, organisasi bahkan dapat mengirimkan pesan darurat kepada semua orang yang berada di lokasi pada hari tersebut.



1. *Praktik Terbaik Keamanan Siber:*

Setelah memastikan keamanan fisik tempat kerja, perhatikan juga keamanan digital. Di era digital seperti sekarang ini, keamanan siber menjadi perhatian utama bagi bisnis. Pada tahun 2022, rata-rata kerugian akibat pelanggaran data mencapai $9,44 juta. Berikut adalah beberapa praktik terbaik terkait keamanan siber di tempat kerja.

2. *Kata Sandi yang Aman*

Karyawan menggunakan berbagai platform dan aplikasi dalam pekerjaan sehari-hari. Mengelola semua kata sandi ini bisa rumit dan berisiko dari segi keamanan. Pertimbangkan untuk menggunakan sistem otentikasi tunggal seperti Okta, yang mengamankan semua kredensial login dalam satu kata sandi utama. Ini membantu menjaga kata sandi karyawan tetap aman dan mengurangi risiko pembobolan.

3. *Pembaruan Perangkat Lunak Secara Rutin*

Memastikan semua perangkat lunak dan sistem operasi Anda diperbarui secara berkala dapat mencegah kerentanan keamanan. Dorong karyawan Anda untuk secara rutin memperbarui perangkat lunak mereka. Berikan pengingat dan bantuan kepada karyawan yang memerlukan bantuan.

4. *Pelatihan Karyawan tentang Ancaman Siber*

Karyawan adalah salah satu lapisan pertahanan utama Anda. Pastikan mereka dilengkapi dengan pengetahuan tentang cara melindungi diri mereka. Selenggarakan sesi pelatihan tentang perlindungan kata sandi, phishing email, dan topik keamanan lainnya. Jadwalkan sesi ini secara teratur dan beri kesempatan untuk bertanya.

5. *Kredensial Wi-Fi yang Unik*

Pengunjung mungkin memerlukan akses Wi-Fi saat mereka berada di kantor. Namun, memberikan akses ini dengan bebas dapat meningkatkan risiko keamanan. Terapkan sistem kredensial Wi-Fi unik untuk setiap pengunjung, mirip dengan yang dilakukan oleh anak perusahaan HP, Aruba. Ini memungkinkan akses internet yang aman untuk pengunjung tanpa risiko yang terlalu tinggi.

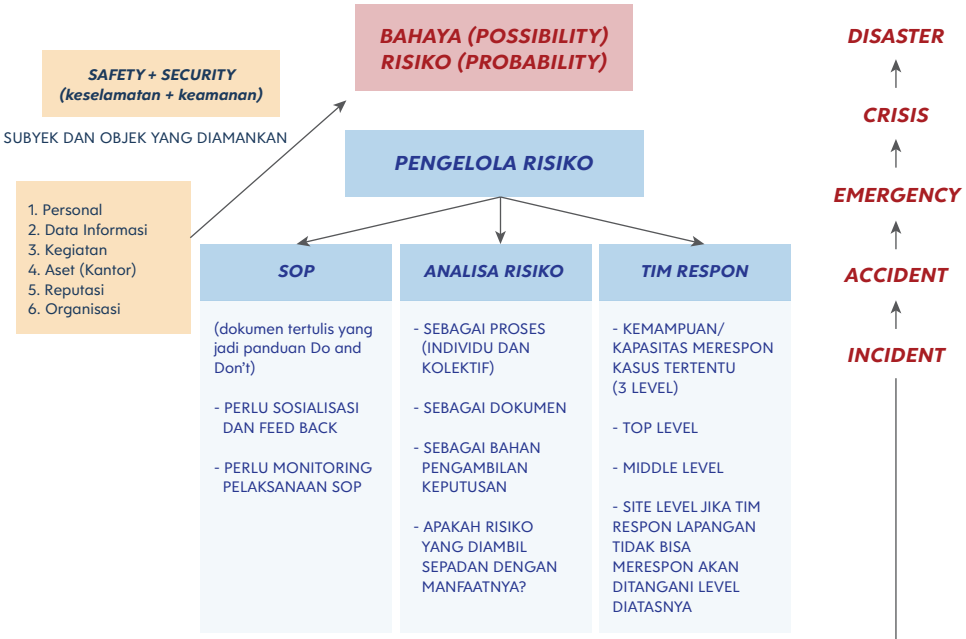
6. *Praktik Terbaik Kesehatan dan Keselamatan*

Kesehatan dan keselamatan karyawan di tempat kerja adalah aspek penting dari keamanan kantor. Mulai dari penyebaran penyakit hingga risiko dari peralatan, pertimbangkan semua faktor yang dapat memengaruhi kesejahteraan karyawan Anda. Berikut beberapa praktik terbaik.:

Verifikasi Kesehatan

Meskipun pandemi mungkin tidak lagi menjadi perhatian utama seperti beberapa tahun yang lalu, tetaplah penting untuk mencegah penyebaran penyakit di tempat kerja. Terapkan alat verifikasi kesehatan atau vaksinasi untuk memastikan karyawan yang masuk telah memenuhi persyaratan kesehatan.

PENGANTAR PENGELOLAAN RISIKO



FUNGSI PENGELOLAAN RISIKO:

1. SEBAGAI LANGKAH PREVENTIF terhadap sesuatu yang AKAN TERJADI yang sifatnya NEGATIF + MERUGIKAN (belum terjadi). MERUGIKAN pada orang, data informasi, kegiatan, aset, reputasi, organisasi.

2. MERESPON sesuatu yang sifatnya NEGATIF dan MERUGIKAN (SUDAH TERJADI)

ANCAMAN: bersumber dari luar dan disengaja terdapat sumber ancaman, bentuk ancaman dan saluran.

KERENTANAN/KERAWANAN: bersumber dari orang, organisasi, lokasi, perlengkapan/ peralatan, aturan

PENGELOLAAN RISIKO: upaya mengontrol/mengendalikan risiko pada tingkat yang bisa diterima oleh individu dan organisasi.

AMAN: RISIKO DAPAT DIKENDALIKAN.

D. Surveillance/Pengawasan

Pembela HAM dan jurnalis kerap menghadapi ancaman saat melakukan kerjanya. Perkembangan teknologi komunikasi dan informasi meningkatkan ancaman terhadap keduanya.

Bagian ini akan membahas pengawasan sebagai salah satu ancaman yang kerap mengikuti pekerjaan pembela HAM dan jurnalis. Secara khusus, pengawasan yang melibatkan teknologi digital akan dibahas pada materi keamanan digital.

Jenis Pengintaian/Pengawasan

Secara umum ada dua jenis pengawasan:

1. Pengawasan terbuka

Adalah pengawasan yang memanfaatkan peralatan yang terlihat dan jelas seperti CCTV, kamera badan, kamera mobil, dan kamera helm.

2. Pengawasan tertutup

Adalah pengawasan yang dijalankan tanpa sepengetahuan objek yang diawasi. Pengawasan seperti ini dapat memanfaatkan kegiatan fisik seperti mengikuti dari jarak tertentu, memotret dan mencatat aktivitas objek hingga pemanfaatan peralatan seperti kacamata, kamera tersembunyi di alat tulis, dasi, dan lainnya

Kedua jenis pengawasan tersebut dapat dibedakan berdasarkan kelompok/orang yang menjalankannya:

PROFESIONAL
Kerja tim
Memanfaatkan kendaraan atau personil di lapangan
Kamera
Melibatkan perencanaan panjang
Targetnya spesifik

AMATIR
Bertindak sendiri
Terlihat intens saat sedang mengintai
Targetnya jangka pendek

// PENTING UNTUK DIKETAHUI

Tahap awal pengintaian adalah pengumpulan informasi. Mereka akan mengikuti, mengamati, dan merekam setiap pergerakan target.

MEREKA INGIN TAHU SEMUANYA TENTANG ANDA.

Mulai dari tempat tinggal, di mana Anda bekerja, rute Anda jalan ke kantor atau pulang ke tempat tinggal, makan di mana, bergaul dengan siapa, dan lainnya. Seluruh informasi tersebut dikumpulkan untuk mendapatkan gambaran pola kegiatan Anda berdasarkan aktivitas harian. Tujuannya, agar pengintai dapat menentukan titik lemah sasarannya sebelum menyerang atau melakukan tindakan.

MEREKA INGIN TAHU SEMUANYA TENTANG ANDA.

Jika Anda melatih kesadaran situasional dengan baik, maka Anda dapat mengantisipasi risiko yang mungkin muncul akibat dari adanya pengawasan terhadap Anda.

Berikut beberapa langkah atau cara yang dapat Anda lakukan guna mengantisipasinya:

1. Terlihat berjalan atau berkegiatan bersama kelompok atau pendamping
2. Menghindari pola yang terlalu jelas dalam aktivitas dan identitas
3. Mengingat atau mencatat detail hal-hal yang rutin terjadi dan terpantau di sekeliling Anda. Selalu peka terhadap segala sesuatu yang tidak rutin atau anomali.
4. Anda sebaiknya memiliki beragam rencana dan sesekali bergerak spontan.
5. Jika Anda merasa diikuti bisa mengambil langkah berbaur dalam kerumunan sembari tidak menggunakan atribut/identitas yang mencolok seperti warna baru, topi, jaket, tas, sepatu, hingga modifikasi kendaraan.
6. Langkah berikutnya jika Anda diikuti dalam konteks lingkungan kota, bisa memanfaatkan pantulan di kaca guna memerhatikan apakah ada yang mengikuti Anda atau tidak.
7. Menyeberang atau melintasi perlintasan jalan dapat memastikan juga apakah ada yang mengikuti Anda atau tidak. Perhatikan jika ada orang yang bereaksi terhadap pergerakan Anda. Mereka yang tampak teragitasi atau tertekan, bisa jadi pengintai Anda.
8. Selalu memeriksa kondisi sekitar sebelum Anda tiba di sebuah lokasi.
9. Tidak mengunggah pesan atau foto secara riil time di media sosial.
10. Tidak mengunggah foto rumah, tempat kerja, tempat parkit, lokasi CCTV, plat nomor kendaraan dan hal lainnya yang memudahkan orang lain mengidentifikasi Anda.

JIKA TERJADI HAL MENCURIGAKAN, segera maksimalkan insting Anda dan lakukan sesuatu mengenai itu.

E. Penahanan vs. Penangkapan

Pembela HAM dan jurnalis kerap harus berhadapan dengan kemungkinan penangkapan atau penahanan. Saat kondisi itu terjadi, sebaiknya tetap tenang agar Anda dapat berpikir jernih sebelum melakukan reaksi atau meresponnya.

Pahami perbedaan antara keduanya. Biasanya, penahanan tidak berlangsung lama. Berbeda dengan penangkapan yang merupakan definisi legal untuk menahan seseorang dan membawanya ke tempat penahanan berdasarkan otoritas, biasanya atas kecurigaan atau tuduhan pidana.

Bagaimana Menghindarinya?

Saat menghadapi penahanan, Anda perlu memastikan siapa yang menahan Anda. Apakah pihak militer, polisi, atau pihak sipil?

Selanjutnya, pastikan apa alasannya, kemungkinan risikonya, serta hak-hak Anda. Upayakan agar Anda tetap tenang hingga bisa bernegosiasi hingga melakukan komunikasi atau malah dibebaskan dari kondisi penahanan.

Saat menghadapi penangkapan, sebaiknya Anda:

- Jangan panik dan tetap tenang
- Berusaha sabar dan tidak memprovokasi
- Berusaha mengingat detil sebanyak mungkin (bahasa, dialek, aroma, suara, lama perjalanan, dll)
- Lakukan semua hal yang bisa menjaga tetap fit dan stabil secara mental
- Terima makanan dan minuman, apa pun yang membantu Anda fit
- Bangun komunikasi dengan mereka agar suasana lebih relax
- Jangan mempercayai ancaman dan janji
- Jangan hilang harapan dan jangan kecewa jika negosiasi tidak berjalan–bisa jadi peluang lepas lebih besar.
- Pertahankan insting Anda dan terus observasi
- Negosiasi untuk bisa berkomunikasi
- Jangan melawan dan berupaya lari, kecuali Anda sangat yakin
- Minta bantuan hukum dari organisasi atau jaringan

Saat menghadapi penangkapan, sebaiknya Anda:

- Bentuk kelompok kerja ad-hoc untuk bereaksi
- Cari tahu lokasi (cek riwayat perjalanan/kegiatan, kontak terakhir, hubungi kontak di lapangan)
- Cari tahu pelaku yang menahan dan apa tujuannya (daftar pendek tersangka)
- Hubungi pihak berwenang (jika memang diperlukan)
- Jangan fokus pada pembuatan kesepakatan tapi upaya nyata untuk melepaskan
- Jika penahanan oleh kelompok bersenjata, kaji kelompoknya dan minta bantuan mediator dari organisasi atau lembaga seperti tetua wilayah, PMI Internasional, gereja, dan lainnya. Penting] berkomunikasi agar tahu alasan penahanan dan upaya pembebasan.
- Pertimbangkan upaya non-litigasi guna memberikan tekanan lebih.
- Beritahu kedutaan atau konsulat jika yang ditahan berasal dari negara lain

F. Mengikuti atau Meliput Demonstrasi dan Protes

Mengikuti aksi protes atau unjuk rasa dapat menimbulkan risiko jika tidak memiliki persiapan. Termasuk juga jurnalis yang hendak meliputnya. Demonstrasi atau protes biasanya melibatkan gerombolan massa.

Untuk meminimalkan risiko dan mencapai hasil yang efektif dengan aman, Anda harus selalu siap. Berikut daftar lengkap pertimbangan Perencanaan dan kebiasaan yang baik untuk membantu kegiatan atau liputan Anda saat demonstrasi atau protes secara aman dan efektif.

Tidak semua akan dapat diterapkan, atau dapat dicapai untuk setiap tugas atau situasi, jadi gunakan dokumen ini sebagai rujukan untuk membantu saat bersiap mengikuti atau meliput agenda tersebut.

Perencanaan penugasan

- **Teliti** faktor pendorong, kelompok utama, hasil peristiwa sebelumnya atau yang serupa, taktik pengunjuk rasa dan pasukan keamanan/kebijakan, senjata anti huru-hara dan senjata yang digunakan oleh pengunjuk rasa/kelompok kriminal, sikap terhadap media.

- **Kebugaran fisik** merupakan pertimbangan penting saat meliput situasi yang tiba-tiba bisa berubah menjadi kekerasan, melakukan penilaian diri/tim, dan memastikan semua orang bugar secara fisik untuk tugas itu.

- Mendapatkan penugasan pada kondisi di atas sangat menuntut **mental**, jadi pikirkan juga keadaan pikiran Anda, pantau diri Anda dan orang lain jika bekerja dalam suatu tim. Pertimbangkan kemungkinan trauma mental setelah tugas.

- **Ketahui undang-undang dan praktik yang relevan** jika penegak hukum atau pengunjuk rasa menuntut untuk memeriksa atau menyita kartu memori atau materi rekaman lainnya.

- **Ketahui area** yang akan Anda kunjungi yaitu pemeriksaan fisik area (tidak selalu ada dan merupakan pilihan), lihat peta, Google Earth, aplikasi navigasi.

- **Jika Anda bepergian dengan kendaraan, jauhkan dari tempat unjuk rasa.**
  Tempatkan di lokasi yang dapat diakses tetapi relatif jauh, sehingga Anda tidak terjebak dalam keriuhan protes dan tidak bisa menjauh.

- **Kenali titik-titik utama** yaitu titik pandang yang dapat dijangkau (platform lebih tinggi lebih disukai), rute keluar dan melarikan diri, titik pertemuan, kemungkinan area yang mungkin berbahaya/kekerasan, fasilitas medis terdekat, dll.

- **Melakukan penilaian risiko** untuk semua jenis risiko dan bahaya untuk semua Langkah penugasan.

- **Buat komunikasi, akuntabilitas, dan rencana darurat** dengan rekan kerja Anda, atau jika bekerja sendiri dengan kontak darurat Anda. Pertimbangkan untuk mengatur grup WhatsApp atau saluran komunikasi aman lainnya, serta dan pertimbangkan apakah bijak

mengatur "lokasi langsung" di ponsel Anda sehingga mereka dapat menemukan Anda jika perlu. Ada aplikasi pelacakan lain yang berguna yaitu "Life 360" yang memungkinkan rekan kerja Anda memantau lokasi Anda dari mana pun mereka berada. Berhati-hatilah dengan aplikasi ini karena membutuhkan paket data yang tidak bisa dipakai dalam demonstrasi besar.

- Jika Anda sendirian, **tentukan titik aman terlebih dahulu** yang jauh dari lokasi aksi. Ketahui akses atau rute untuk menghindari kericuhan saat terjadi, hingga toko, bangunan, atau hunian yang dapat dijadikan lokasi perlindungan sementara.

- **Cetak peta**, atau cetak citra Google Earth, peta luring.

- **Unduh peta offline ke ponsel** sehingga masih dapat dipakai jika jaringan ponsel mati atau "macet".

- Pastikan **baterai ponsel Anda penuh**. Kenali area yang akan Anda tuju. Tetapkan terlebih dahulu apa yang harus dilakukan dalam keadaan darurat.

- Cobalah sedapat mungkin bekerja dengan rekan kerja dan lakukan memiliki **prosedur pelaporan secara berkala dengan titik kontak darurat utama Anda**, terutama saat meliput rapat umum atau acara unjuk rasa yang ramai.

- Jika Anda memiliki **Kartu Pers**, putuskan apakah bijak untuk menunjukkannya atau menyembunyikannya.

- **Pakaian harus dipilih dengan cermat,** termasuk apakah akan lebih menonjol terlihat atau berbaur (hindari pakaian bergaya militer). Pakai pakaian berlapis, dan alas kaki yang memungkinkan Anda bergerak cepat, dengan sol anti selip juga penting dipertimbangkan.

- **Hindari memakai kalung, kuncir kuda, tali leher,** atau apa pun yang bisa ditarik, **serta bahan yang mudah terbakar,** seperti nilon.

- **Pasang dan periksa semua Alat Pelindung Diri** dan pastikan masker gas dan respirator memiliki segel kedap udara di wajah Anda. Jangan gunakan alat perlindungan diri saat kegiatan aksi baru dimulai karena dapat memicu kemarahan peserta aksi karena mengira aksinya bakal berlangsung ricuh.

- **Bawalah peralatan medis,** dan **senter kepala** atau senter kecil jika bekerja di malam hari.

- Jika bepergian dengan kendaraan, **bawa pakaian cadangan dan kantong sampah plastik,** jadi jika pakaian Anda terkontaminasi (paparan gas air mata), Anda dapat mengganti dan memasukkan pakaian yang terkontaminasi ke dalam kantong sampah plastik dan mengikatnya di bagasi kendaraan.

- **Ambil air dan makanan ringan** (yaitu peras beberapa jus jeruk ke dalam air Anda karena ini dapat membantu menghilangkan kontaminasi gas air mata/gas CS atau semprotan merica.

- **Membawa selendang atau saputangan** berguna untuk mengatasi kadar rendah gas air mata atau untuk mengeringkan wajah setelah penggunaan *water canon.*

- Karena Anda tidak mengetahui berapa lama kegiatan demonstrasi berlangsung jika terjadi sesuatu di luar kebiasaan,

pikirkan untuk membawa:

1. ***Air atau minuman pengganti elektrolit***
2. ***Buah kering (untuk mendapatkan glukosa sesegera mungkin) atau protein batangan.***
3. ***Baterai cadangan***
4. ***Kotak P3K***
5. ***Tissue***
6. ***Senter kepala, vital jika demonstrasi berlangsung hingga malam***
7. ***Tetes mata***

- **Batasi barang berharga** yang Anda miliki, ambil seperlunya.

Mendampingi Demonstrasi atau Unjuk Rasa

- Pertimbangkan selalu posisi Anda. Jika memungkinkan, cobalah untuk menemukan posisi yang lebih tinggi yang dapat memberikan keamanan yang lebih besar.

- Di setiap lokasi, selalu tentukan jalur evakuasi. Jika bekerja dengan orang lain, pilih titik dan prosedur pertemuan darurat yaitu "jika kita terpisah selama 20 menit bertemu di lokasi ini".

- Selalu pertahankan kesadaran situasional dan ingat setelah gelap risiko Tindakan kriminal meningkat.

- Jika bekerja di keramaian, rencanakan strategi. Cobalah untuk tetap berada di luar kerumunan dan menghindari berada di tengah-tengah kerumunan karena sulit melarikan diri. Selalu kenali rute pelarian.

- Jika Anda berada di antara kerumunan unjuk rasa sebelum mengenali titik rujukan ke rute pelarian, hitung waktu berada di sana kemudian mundur ke samping, evaluasi kembali dan kemudian jika Anda perlu kembali lagi ke kerumunan. Lanjutkan proses ini karena akan memastikan Anda membatasi paparan Anda ke area berisiko tinggi serta mempertahankan kesadaran situasional tentang apa lagi yang terjadi di sekitar.

- Saat meliput protes kekerasan, Anda harus memutuskan apakah akan memosisikan diri di pihak pengunjuk rasa atau pihak berwenang. Keputusan ini akan menentukan paparan ancaman Anda, bergantung pada tindakan kedua belah pihak. Hindari sedapat mungkin berakhir berada di tengah-tengah di antara pengunjuk rasa dan pihak berwenang; ini adalah lokasi paling berbahaya.

- Kerumunan besar menciptakan potensi risiko kekerasan seksual. Wartawan harus selalu bekerja dengan rekan kerja dan memiliki sarana untuk membunyikan alarm. Bekerja setelah gelap jauh lebih berisiko dan sedapat mungkin harus dihindari.

- Guna menghindari kekerasan seksual, sebaiknya membawa peluit agar bisa segera ditiup jika memerlukan bantuan.

- Pantau tanda-tanda kekerasan seperti ketegangan yang meningkat, pengunjuk rasa muncul dalam kelompok dengan wajah tertutup, perubahan formasi atau tindakan polisi atau militer. Dalam situasi yang dinamis, terus evaluasi ulang strategi keluar Anda. Percayai insting

Anda dan buat keputusan positif kapan saatnya untuk pergi!

- Ingat rencana pertanggungjawaban Anda dan hubungi kontak darurat Anda sesuai rencana.

- Sadarilah akan materi yang Anda pegang di perangkat, unduh perangkat sesering mungkin. Ambil kartu memori cadangan dan ganti secara berkala. Unduh rekaman harian di akhir setiap hari dan mulai lagi keesokan harinya dengan kartu kosong.

- Wartawan harus mematuhi perintah dari petugas penegak hukum, meskipun pihak berwenang terkadang menangkap wartawan tanpa memberi perintah terlebih dahulu.

- Nilai sendiri keadaan pikiran Anda, ini adalah lingkungan yang sangat stres dan stres dapat menumpuk selama periode waktu yang lama. Jika Anda merasa cemas atau stres, bicaralah dengan rekan kerja, teman dekat, atau mencari nasihat profesional.

Dalam situasi di mana gas air mata mungkin digunakan:

- Bahan pengendali huru-hara dirancang agar bereaksi dengan uap air sehingga menyebabkan sensasi terbakar. Mata, tenggorokan, dan hidung sangat berisiko. Dampaknya biasanya hilang setelah kira-kira satu jam, tetapi kulit mungkin tetap teriritasi selama berjam-jam. Gas air mata menyerang paru-paru. Jadi jika Anda menderita penyakit pernapasan seperti asma, Anda harus mempertimbangkan apakah Anda harus terpapar. Gas air mata lebih berat daripada udara, sehingga sering berada tepat di atas tanah jika tidak ada angin untuk membubarkannya. Jika dipakai dalam konsentrasi tinggi, terutama di daerah yang padat bangunan, gas bisa menimbulkan bahaya kesehatan yang serius.

- Memakai alat pelindung diri, termasuk masker gas, pelindung mata, dan helm, pelindung tubuh juga disarankan jika ada.

- Lensa kontak tidak disarankan dipakai, kacamata lebih disukai (lensa polikarbonat resistensi yang diperoleh dengan resep dapat dibuat khusus agar sesuai dengan bingkai kacamata pengaman oleh tukang kacamata, bergantung keadaan Anda). Jika memakai kacamata biasa, pastikan kacamata itu pas di bawah masker gas Anda, dan kacamata pengaman ini bisa muat di atasnya dengan segel kedap udara.

- Bagi yang mengidap asma atau masalah pernapasan harus menghindari area tempat gas air mata digunakan. Saat gas air mata banyak digunakan, ada kemungkinan konsentrasi gas yang tinggi berada di area tanpa pergerakan udara.

- Catat dan ingat bangunan penting yang mudah dikenali (yaitu tiang, trotoar) yang dapat digunakan untuk membantu Anda memandu keluar dari suatu area jika Anda kesulitan melihat.

- Pertimbangkan untuk menyiapkan "zona panas" saat Anda kembali dari tugas. Zona panas adalah area tempat Anda mendekontaminasi peralatan dan melepaskan pakaian yang

terkontaminasi, dll. sebelum pindah ke area bersih. Tempatkan pakaian yang terkontaminasi ke dalam mesin cuci, atau ke dalam kantong tertutup, cuci tangan/wajah Anda.

- Mandi sesegera mungkin, pertama gunakan air dingin lalu hangatkan.

- Hari-hari bisa jadi sangat panjang dan melelahkan, saat Anda selesai pastikan Anda banyak minum dan makan, istirahatlah sebanyak mungkin.

- Jika Anda terkena gas air mata, cobalah menemukan tempat yang tinggi, dan berdiri melawan angin di udara segar agar angin menghalau gas ini. Jangan menggosok mata atau wajah Anda. Bilas mata Anda – miringkan kepala dengan mata yang sedang memerah menghadap ke bawah, dan siram dari dalam ke luar, sehingga air menetes menjauhi wajah.

- Saat Anda menemukan tempat mandi, mandilah dengan air dingin mancur untuk membersihkan gas dari kulit Anda, tetapi jangan menggosok tubuh. Pakaian mungkin perlu dicuci beberapa kali agar kristal sepenuhnya hilang.

Saat menghadapi agresi:

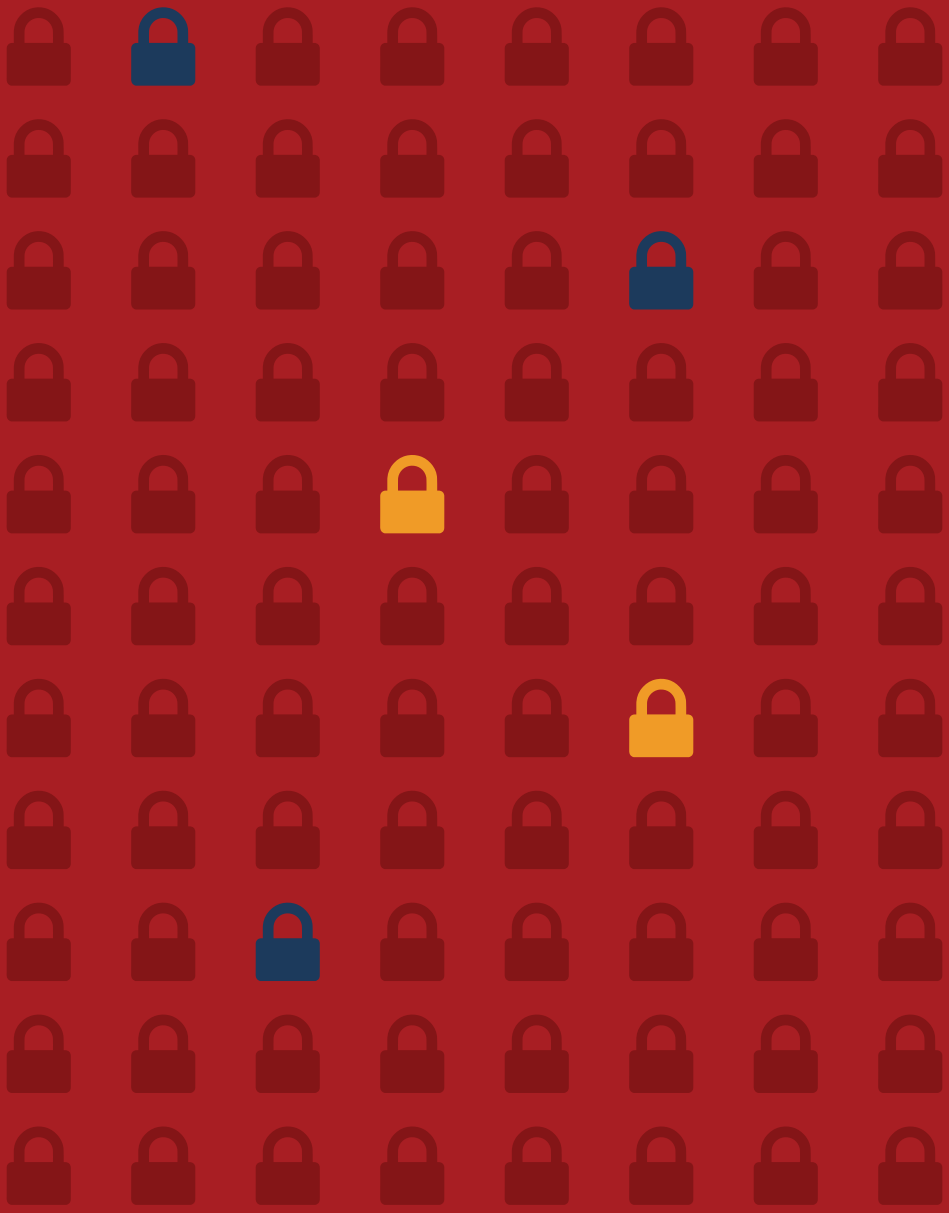
- Baca bahasa tubuh dan gunakan bahasa tubuh Anda sendiri untuk menenangkan situasi, jaga kontak mata dengan gerakan tangan terbuka, dan sikap yang tidak mengancam/agresif dan tetap berbicara dengan cara yang menenangkan.

- Menjauhlah sepanjang tangan Anda dari ancaman, coba dan kenali jalan keluar dan mundur dan jika seseorang memegang Anda, lepaskan dengan kuat tanpa agresi. Jika terpojok dan dalam bahaya, berteriaklah. Peluit atau alarm pemerkosaan mungkin berguna untuk mengalihkan atau membingungkan penyerang sehingga Anda dapat melarikan diri jika mereka terlalu dekat.

- Jika situasinya memanas, bebaskan tangan Anda untuk melindungi kepala dan bergeraklah dengan langkah-langkah pendek yang disengaja agar tidak jatuh. Jika bersama tim, tetap bersatu, dan bergandengan tangan.

- Selalu waspada terhadap situasi dan keselamatan sendiri. Meskipun terkadang mendokumentasikan agresi bisa menjadi berita, memotret individu yang agresif dapat memanaskan situasi jadi selalu waspadalah terhadap "efek kamera".

- Tetap tenang jika Anda ditangkap. Jika Anda memilih menolak petugas yang menangkap, Anda dapat memperburuk situasi. Jika Anda benar-benar berbicara, berusahalah keras untuk mempertahankan sikap profesional saat menjelaskan bahwa Anda adalah seorang jurnalis yang meliput berita. (Apa pun simpati yang mungkin Anda miliki bagi setiap pelaku di lapangan tidak penting; yang selalu penting adalah bahwa seorang pendamping atau jurnalis bertindak di lapangan bukan sebagai peserta tetapi sebagai pengamat.) Jika pihak berwenang memutuskan untuk melanjutkan penangkapan, patuhi perintah dan tunggu kesempatan untuk menjelaskan masalah Anda dengan tenang kepada atasan pihak yang berwenang.



kemitraan partnership

SAFEnet

www.safenet.or.id

@safenetvoice

09
24

P3IK: Pertolongan Pertama Pada Insiden Keamanan

MODUL PENANGANAN INSIDEN KEAMANAN UNTUK PPHAM DAN OMS