Norwegian Embassy
Jakarta

humanis
igniting agency, inspiring change

PANDUAN KEAMANAN HOLISTIK UNTUK PEREMPUAN / PEMBELA HAM [WOMAN / HUMAN RIGHTS DEFENDERS]

BUKU SAKU

PANDUAN KEAMANAN HOLISTIK UNTUK PEREMPUAN/ PEMBELA HAM [WOMEN/ HUMAN RIGHTS DEFENDERS]

BUKU SAKU PANDUAN KEAMANAN HOLISTIK UNTUK PEREMPUAN/ PEMBELA HAM [W/HRDS]

Penulis

An Nisaa Yovani, Ellen Kusuma

Kontributor

Andra Ferdinand, Radhina Fasya Tazkianida

Penyunting

Ni Loh Gusti Madewanti

Desain dan Tata Letak

Muhammad Rizki, Taufiqurahman Kifu

Penerbit

Yayasan Humanis dan Inovasi Sosial
18 Office Park, lantai 15, Unit B JL T.B Simatupang No.18 Jakarta Selatan 12520 Indonesia
Telp: 021 2787 6233 Fax: 021 2787 6242

Website: https://humanis.foundation
Instagram: @humanisfoundation
Twitter: @hsi_foundation
Facebook Page: Humanis Foundation

Penafian

Buku saku ini merupakan salah satu keluaran dari kegiatan Lokakarya Keselamatan dan Keamanan Holistik bagi Perempuan/ Pembela HAM, berkolaborasi dengan *Holistic Security Feminist project* antar *impact area Civil Rights in Digital Era* **(CRIDA)** dan *Gender, Equality, Diversity and Inclusion* **(GEDI).**

Buku saku ini diproduksi oleh Yayasan Humanis dan Inovasi Sosial atas dukungan pendanaan dari *The Norwegian Embassy to Indonesia and Timor-Leste* di bawah *project* Percepatan dan Penguatan Advokasi Aturan Turunan Undang-Undang Tindak Pidana Kekerasan Seksual. Materi dalam publikasi ini adalah semata-mata tanggung jawab dari Yayasan Humanis dan Inovasi Sosial dan tidak otomatis mencerminkan pandangan dari *The Norwegian Embassy to Indonesia and Timor-Leste.*

Publikasi pertama Oktober 2024

PENGANTAR

Tidak disangka, Senin 24 Juni 2024, Polda DIY menetapkan Meila Nurul Fajriah sebagai Tersangka pencemaran nama baik sesuai dengan pasal 27 ayat (3) UU ITE jo Pasal 45 Ayat (3) UU ITE. Penetapan ini bermula saat Meila melakukan pendampingan kasus Kekerasan Seksual di Yogyakarta sejak April 2020. Meila adalah Pengacara LBH Yogyakarta yang melakukan pembelaan terhadap 30 korban kekerasan seksual baik langsung maupun secara online yang diduga kuat dilakukan oleh satu pelaku yakni IM (mantan Mahasiswa berprestasi Universitas Islam Indonesia). Apa yang terjadi kepada Meila merupakan serangan serius terhadap Perempuan Pembela HAM yang sedang mendampingi korban. Kejadian ini juga merupakan upaya sistematis Polda DIY melindungi terduga Pelaku Kekerasan Seksual.

Kriminalisasi termasuk *Judicial Harassment,* kekerasan psikis, fisik, serangan digital dan bahkan kematian adalah risiko yang harus dihadapi oleh para Pembela HAM (*Human Rights Defenders*). Perempuan Pembela HAM dan pembela HAM dari kelompok gender dan seksualitas yang beragam masuk dalam kelompok paling rentan dan menghadapi risiko tinggi (Komnas Perempuan, 2023).

Sejak beralihnya rezim pada tahun 1998, masa reformasi dan bahkan sepuluh tahun terakhir kepemimpinan

Presiden Joko Widodo, serangan terhadap para pembela HAM tidak mengalami penurunan. Selimut kekebalan masih melindungi para pelaku dari jeratan hukum, sehingga kondisi Pembela HAM bahkan selama paska reformasi tidak otomatis bertambah baik. Pola-pola serangan terhadap Pembela HAM justru menunjukan peningkatan kualitas disertai semakin beragamnya aktor pelaku kekerasan. Jika pada masa Soeharto peranan aktor negara seperti aparat kepolisian, militer, intelejen dan sipil birokrat sangat dominan, maka pada masa sekarang ini muncul aktor-aktor non-negara yang di-*back up* oleh negara, misalnya kelompok-kelompok preman, kelompok-kelompok milisi bersenjata, kelompok-kelompok fundamentalis.

Selain harus menghadapi serangan dari para aktor pelaku kekerasan, para Pembela HAM juga harus menghadapi jeratan perangkat hukum dan perundang-undangan lainnya yang juga digunakan sebagai senjata mengkriminalkan mereka. Ketika jaman Soeharto, para pembela HAM harus menghadapi jeratan UU Subversi dan pasal-pasal karet KUHP, maka saat ini Pembela HAM harus menghadapi kriminalisasi UU ITE dengan ancaman penangkapan dan penahanan sewenang-wenang. Belum usai hak korban terpenuhi, pendampingnya juga rentan

terkena dampak kesehatan fisik, mental dan sosial, serta potensi kriminalisasi dari pasal-pasal karet UU ITE atau ancaman dan kerentanan lainnya di *platform digital.*

Laporan Akhir Tahun 2023 (CATAHU 2023) mencatat jumlah kasus kekerasan terhadap perempuan di ranah negara meliputi kasus kekerasan terhadap perempuan/ pembela hak asasi manusia (W/HRDs), kekerasan terhadap perempuan dan kelompok gender dan seksualitas beragam oleh anggota POLRI/TNI, pengusiran paksa, penyiksaan, dan perlakuan tidak manusiawi dan merendahkan martabat berdasarkan gender, kebijakan diskriminatif, kebebasan beribadah dan beragama, tempat tinggal, dan administrasi kependudukan.

Menyadari risiko tinggi yang harus dihadapi para Pembela HAM di seluruh dunia, maka Majelis Umum Perserikatan Bangsa-Bangsa pada 9 Desember 1998 sebenarnya telah mengeluarkan Resolusi Nomor 53/144 yang mengesahkan Deklarasi Hak dan Tanggung Jawab Perseorangan, Kelompok dan Seluruh Masyarakat untuk Mempromosikan dan Melindungi Hak Asasi Manusia dan Kebebasan-kebebasan Dasar yang diakui secara universal *(Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote*

and Protect Universally Recognized Human Rights and Fundamental Freedoms). Deklarasi ini kemudian dikenal dengan **Deklarasi Pembela HAM.** Dalam konstitusi Undang-Undang Dasar 1945-pun telah menjamin bahwa hak asasi manusia meliputi perlindungan dari berbagai bentuk kekerasan berbasis gender, termasuk kekerasan seksual, hak atas keselamatan individu, hak atas kebebasan dan keamanan pribadi, dan hak untuk membela diri atas kehormatan dan martabat seseorang.

Namun Para Pembela HAM lagi-lagi menjadi target serangan karena aktivitasnya yang memperjuangkan, mempromosikan dan membela hak-hak asasi manusia, terutama mereka yang selama ini dipinggirkan dan disingkirkan. Oleh karena itu perlindungan terhadap Pembela HAM sangat mutlak diperlukan. Berdasarkan kewajiban internasional, maka negara adalah yang paling berkewajiban untuk menjaga keselamatan Pembela HAM. Akan tetapi realitasnya negara yang justru seringkali melakukan pelanggaran atau lalai menjamin keselamatan Pembela HAM. Oleh karena itu, Pembela HAM perlu membekali diri dengan pengetahuan dan keterampilan agar bisa menjaga keselamatannya demi keberlangsungan penegakan HAM.

Humanis sebagai organisasi yang memfokuskan pada pemenuhan dan terwujudnya Hak Asasi Manusia, didukung oleh *The Norwegian Embassy to Indonesia and Timor-Leste* mencoba memproduksi dan menerbitkan buku saku ini yang berisi informasi dan panduan bagi Perempuan/ Pembela HAM.

Bagian buku saku ini terdiri dari beberapa informasi sangat penting dan berguna untuk para Pembela HAM membekali diri, meliputi **Pengenalan Keamanan Holistik dan Privasi; Perihal Kasus-Kasus Rekayasa Sosial; Bagaimana Cara Melakukan Assesmen Resiko** dan **Kesadaran Situasi; Bagaimana Cara Merawat Diri** dan **Apa Itu Perawatan Kolektif; Bagaimana Cara Memberikan Pertolongan Dasar Holistik; Tahapan Komunikasi Aman;** dan **Mekanisme Penanganan** dan **Rujukan Laporan**.

Kami mengucapkan terima kasih kepada semua kawan Pembela HAM termasuk Perempuan dan kelompok keragaman gender dan seksualitas yang telah terlibat pada Lokakarya Keselamatan dan Keamanan Holistik, yang membantu memperkaya buku ini. Kawan-kawan Pembela HAM yang terlibat dalam Lokakarya tersebut telah meluangkan waktu untuk berkenan berbagi

pengalaman kasus yang mereka tangani, termasuk resiko yang pernah dihadapi di daerah yang masih menerapkan peraturan diskriminatif, upaya menghadapi masyarakat dengan kultur yang patriarkis serta misoginis, jeratan berbagai aturan hukum melalui pasal-pasal karet yang berpotensi mengkriminalisasi para pembela HAM.

Buku saku ini juga merupakan bekal pengetahuan dari banyak pembelajaran dan cerita sukses, advokasi sebagai strategi resiliensi bertahan dan melawan tirani. Akhir kata, kami berharap semoga buku ini dapat bermanfaat dan mendorong pemenuhan perlindungan Perempuan – Pembela HAM di Indonesia [W/HRDs].

Jakarta, Oktober 2024

Tunggal Pawestri
Direktur Eksekutif Yayasan Humanis dan Inovasi Sosial

DAFTAR ISI

1
Tujuan

Tujuan dari buku saku ini adalah untuk memperkenalkan konsep keamanan holistik kepada para pembela hak asasi manusia (HAM) dan para profesional yang bekerja di bidang bantuan hukum dan kemanusiaan. **Buku ini akan memberikan pemahaman mendalam tentang tiga jenis utama keamanan holistik: digital, fisik, dan psikososial, serta menjelaskan bagaimana ketiga aspek keamanan ini saling terkait dan mempengaruhi satu sama lain.** Pentingnya keamanan holistik terletak pada kenyataan bahwa setiap aspek dari keamanan tidak bisa berdiri sendiri, melainkan harus dipahami sebagai bagian dari sebuah sistem yang saling terhubung. Bagi pembela HAM, pengetahuan tentang keamanan holistik sangatlah krusial karena memungkinkan mereka untuk memberikan bantuan kepada korban dengan perspektif yang lebih menyeluruh dan komprehensif, yang pada akhirnya akan meningkatkan efektivitas dukungan yang diberikan.

Selain itu, **buku saku ini juga bertujuan untuk menjelaskan mekanisme pelaporan kasus yang dapat dijadikan rujukan oleh lembaga-lembaga yang menyediakan layanan bantuan maupun oleh lembaga-lembaga yang hendak mengakses layanan tersebut.** Dengan mengetahui mekanisme

ini, diharapkan para profesional dapat mengukur dan mempersiapkan segala sesuatu yang dibutuhkan dengan lebih baik, sehingga proses pelaporan dan penanganan kasus dapat berjalan dengan lebih efektif dan efisien.

Terakhir, buku ini akan menyajikan panduan praktis mengenai hal-hal apa saja yang harus diperhatikan dan diukur oleh setiap lembaga, serta langkah-langkah persiapan yang diperlukan untuk memastikan bahwa layanan yang diberikan sesuai dengan standar keamanan holistik. Dengan demikian, buku saku ini diharapkan dapat menjadi alat yang berguna untuk meningkatkan kapasitas dan kesiapan lembaga-lembaga dalam menghadapi berbagai tantangan keamanan yang ada.

2

Perkenalan Terhadap Keamanan Holistik

Apa itu keamanan holistik?

Keamanan holistik adalah pendekatan yang menyatukan berbagai aspek keamanan untuk memastikan perlindungan menyeluruh bagi individu atau kelompok. Pendekatan ini tidak hanya berfokus pada satu aspek tertentu, tetapi mencakup keamanan digital, fisik, dan psikososial, yang semuanya saling terkait dan mempengaruhi kesejahteraan keseluruhan seseorang.

Kenapa sekarang kita membicarakan keamanan holistik?

Di era modern ini, ancaman terhadap keamanan tidak hanya datang dari satu sumber saja. Pekerjaan dalam bidang hak asasi manusia atau jurnalisme, misalnya, menuntut individu untuk bekerja di bawah tekanan tinggi dan sering kali di lingkungan yang berisiko. Ancaman dapat bersifat digital seperti peretasan, fisik seperti kekerasan atau intimidasi, dan psikososial seperti stres atau *burnout*. Karena itu, pendekatan keamanan holistik menjadi sangat penting untuk memastikan bahwa semua aspek keamanan dikelola dengan baik, sehingga dapat memberikan perlindungan yang lebih efektif dan menyeluruh.

Bagaimana cara keamanan holistik bekerja?

Keamanan holistik bekerja dengan mengidentifikasi dan mengelola risiko-risiko yang ada di berbagai aspek kehidupan seseorang. Ini melibatkan evaluasi dan penerapan langkah-langkah perlindungan di bidang digital, fisik, dan psikososial. Pendekatan ini mengakui bahwa setiap individu memiliki kebutuhan yang unik dan oleh karena itu, langkah-langkah perlindungan harus disesuaikan dengan konteks pribadi dan profesional mereka. Dengan mengintegrasikan berbagai bentuk perlindungan, pendekatan ini memastikan bahwa keamanan tidak hanya terfokus pada satu aspek, tetapi mencakup semua area yang berpotensi menimbulkan risiko.

Aspek apa saja yang ada di bawah keamanan holistik?

1. Keamanan Digital: Meliputi perlindungan terhadap data dan informasi pribadi, penggunaan alat dan aplikasi yang aman, manajemen kata sandi, serta pemahaman tentang ancaman siber seperti peretasan dan *phishing*.

2. Keamanan Fisik: Meliputi perlindungan terhadap ancaman fisik seperti kekerasan atau intimidasi,

keamanan tempat kerja, serta prosedur keselamatan saat bepergian.

3. Kesejahteraan Psikososial: Meliputi dukungan terhadap kesehatan mental dan emosional, manajemen stres, serta mekanisme untuk mengatasi *burnout* dan tekanan pekerjaan yang berlebihan.

Pendekatan holistik ini menekankan pentingnya keseimbangan dan integrasi antara ketiga aspek ini untuk memastikan perlindungan yang maksimal dan kesejahteraan yang berkelanjutan bagi individu maupun kelompok yang rentan terhadap berbagai bentuk ancaman.


KARTU TANDA PENDUDUK


KARTU TANDA PENDUDUK

3

Pengenalan Terhadap Privasi

Apa itu Privasi?

Privasi adalah hak atau kemampuan individu untuk mengendalikan informasi pribadi mereka dan menentukan bagaimana informasi tersebut dikumpulkan, digunakan, dan dibagikan. Privasi mencakup berbagai aspek, termasuk data pribadi, percakapan pribadi, serta aktivitas *online* dan *offline* seseorang. Dalam konteks digital, Privasi sering kali mengacu pada perlindungan data pribadi dari akses yang tidak sah dan pengawasan. Misalnya, ketika Anda mengatur profil media sosial menjadi "*private*" maka Anda sedang mengontrol siapa yang dapat melihat informasi dan aktivitas Anda.

Video: *https://www.instagram.com/REEL/CUYJBLOMSAN/@digitallytante*

Bagaimana Privasi bekerja?

Privasi bekerja melalui berbagai mekanisme yang dirancang untuk melindungi informasi pribadi dari akses yang tidak sah dan penggunaan yang tidak sesuai. Ini termasuk enkripsi data,

penggunaan kata sandi yang kuat, pengaturan privasi di media sosial, dan kebijakan privasi yang ketat oleh penyedia layanan. Selain itu, Privasi juga melibatkan hak individu untuk memberikan atau menolak izin (konsen) terhadap pengumpulan dan penggunaan data mereka. Contoh: Ketika Anda berbelanja *online*, informasi kartu kredit Anda dienkripsi untuk mencegah pencurian data. Anda juga dapat mengatur siapa yang dapat melihat postingan Anda di media sosial.

Kenapa kita butuh Privasi?

Privasi penting karena melindungi hak individu untuk menjaga kerahasiaan informasi pribadi mereka. **Tanpa Privasi, data pribadi dapat disalahgunakan untuk tujuan yang merugikan, seperti pencurian identitas, diskriminasi, atau pengawasan yang tidak sah. Privasi juga mendukung kebebasan berekspresi dan kebebasan berkumpul, karena individu dapat merasa aman untuk berbagi pendapat dan berpartisipasi dalam kegiatan sosial tanpa takut akan reperkusi.** Misalnya, tanpa perlindungan privasi, data kesehatan Anda bisa digunakan oleh perusahaan asuransi untuk menolak klaim atau menaikkan premi tanpa sepengetahuan Anda.

Kapan Privasi dibutuhkan?

Privasi dibutuhkan setiap saat, terutama saat seseorang berkomunikasi, berbagi informasi, atau melakukan aktivitas yang melibatkan data pribadi. Ini termasuk penggunaan internet, media sosial, *email*, layanan perbankan *online*, serta dalam kehidupan sehari-hari seperti percakapan pribadi dan transaksi keuangan. Privasi juga sangat penting dalam konteks pekerjaan, terutama bagi mereka yang bekerja di bidang yang melibatkan data sensitif, seperti kesehatan, hukum, dan hak asasi manusia. Contoh: Saat mendaftar akun *email*, Anda memberikan informasi pribadi yang perlu dilindungi dari akses yang tidak sah.

Siapa yang membutuhkan Privasi?

Setiap individu membutuhkan Privasi, terlepas dari usia, jenis kelamin, profesi, atau status sosial. Privasi adalah hak dasar yang diakui secara universal dan diperlukan untuk melindungi martabat serta kebebasan individu. Organisasi juga membutuhkan Privasi untuk melindungi data perusahaan dan informasi sensitif terkait klien atau pelanggan mereka. Misalnya, seorang jurnalis membutuhkan privasi untuk melindungi sumber informasi mereka, sedangkan seorang remaja

membutuhkannya untuk menjaga keamanan informasi pribadi mereka di media sosial.

Konsen, berkaitan dengan ketubuhan kita:

Konsen (persetujuan) adalah aspek penting dari Privasi, terutama dalam konteks bagaimana informasi pribadi dikumpulkan dan digunakan. **Konsen berarti individu memberikan izin secara sadar dan sukarela sebelum data mereka dikumpulkan atau digunakan oleh pihak lain.** Ini berkaitan erat dengan hak individu untuk mengendalikan informasi pribadi mereka dan memastikan bahwa data mereka tidak disalahgunakan. Contoh: Saat mengunduh aplikasi kesehatan, Anda mungkin diminta untuk memberikan izin agar aplikasi dapat mengakses data kesehatan Anda seperti detak jantung atau aktivitas fisik.

Konsen juga penting dalam konteks ketubuhan kita, di mana individu memiliki hak untuk memberikan atau menolak izin terhadap penggunaan data atau informasi yang berkaitan dengan tubuh dan kesehatan mereka, termasuk dalam penelitian medis atau layanan kesehatan.

Privasi dan Tubuh Digital:

Tubuh digital adalah representasi dari identitas seseorang di dunia maya, yang terdiri dari semua data pribadi dan aktivitas *online* mereka. Privasi membantu melindungi tubuh digital dengan membatasi akses dan penggunaan data ini. Misalnya, mengontrol siapa yang dapat melihat lokasi Anda, mem*posting* di media sosial, atau mengakses riwayat pencarian Anda adalah cara untuk melindungi tubuh digital Anda.

Hubungan dengan Jejak Digital:

Jejak digital atau *digital footprint* adalah jejak data yang ditinggalkan seseorang saat mereka menggunakan internet. Ini mencakup segala sesuatu mulai dari situs web yang dikunjungi, email yang dikirim, postingan media sosial, hingga pembelian *online*.

Hubungan antara Privasi, Perlindungan Identitas, dan *Digital Footprint*:

Pengumpulan Data:

Privasi mengatur bagaimana data dikumpulkan dan digunakan oleh pihak ketiga. Misalnya, kebijakan privasi pada situs web menjelaskan bagaimana data pengguna akan dikelola. Setiap aktivitas *online* meninggalkan jejak

digital. Semakin banyak data yang dikumpulkan, semakin besar jejak digital seseorang.

Pengendalian Data:

Melalui pengaturan privasi, individu dapat mengontrol apa yang dibagikan dan kepada siapa. Ini termasuk mengatur siapa yang dapat melihat postingan media sosial atau memilih untuk tidak dilacak oleh situs web. Dengan mengelola pengaturan privasi, individu dapat meminimalkan jejak digital mereka, misalnya dengan menggunakan mode penyamaran saat *browsing* atau menghapus riwayat pencarian secara berkala.

Keamanan Data:

Proteksi terhadap akses yang tidak sah dan penyalahgunaan data pribadi melalui enkripsi dan autentikasi dua faktor sangat penting. Jejak digital yang tidak terkelola dengan baik dapat mengarah pada pencurian identitas atau penipuan. Menjaga keamanan data berarti melindungi informasi yang membentuk jejak digital Anda.

Dampak Jangka Panjang:

Melindungi Privasi memastikan bahwa data pribadi tidak digunakan tanpa izin untuk tujuan yang merugikan.

Jejak digital dapat memiliki dampak jangka panjang pada reputasi seseorang. Informasi yang dipublikasikan secara *online* bisa sulit dihapus dan dapat mempengaruhi peluang kerja, hubungan pribadi, dan lainnya.

Contoh Praktis:

- Penggunaan Media Sosial: Mengatur akun media sosial menjadi privat agar hanya teman yang bisa melihat postingan Anda. Setiap postingan, *like*, dan komentar menjadi bagian dari jejak digital Anda yang bisa diakses di masa depan.
- Belanja *Online*: Menjaga informasi kartu kredit tetap aman dengan menggunakan situs web yang terenkripsi. Riwayat pembelian Anda bisa digunakan oleh perusahaan untuk profil pemasaran.
- Pencarian di Internet: Menggunakan mesin pencari yang menghormati Privasi, seperti *DuckDuckGo*. Riwayat pencarian Anda disimpan oleh mesin pencari dan bisa digunakan untuk profil iklan atau analisis.

Dengan memahami dan mengelola Privasi, individu dapat lebih baik melindungi identitas mereka dan mengurangi risiko yang terkait dengan jejak digital mereka.


Anak
2
30th
Jl. Sadrah
No.5
Bandung
Reka
PNS

4

Siapa yang Rentan Terkena Rekayasa Sosial

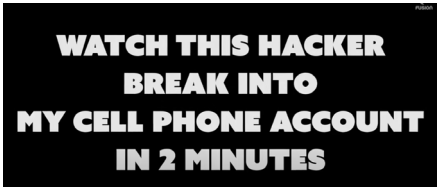
Setiap orang dapat menjadi target rekayasa sosial, tetapi mereka yang memiliki akses ke informasi sensitif atau posisi berpengaruh lebih rentan. Individu yang kurang sadar akan praktik keamanan digital dan tidak waspada terhadap tanda-tanda manipulasi juga merupakan target yang mudah. Selain itu, orang-orang yang sering berbagi informasi pribadi di media sosial atau yang memiliki kebiasaan *online* yang tidak aman lebih rentan terhadap serangan ini.

Bagaimana rekayasa sosial bekerja?

Rekayasa sosial bekerja melalui serangkaian tahapan:

1. **Investigasi:** Penyerang mengidentifikasi dan mengumpulkan informasi tentang target mereka, sering kali melalui pengawasan atau penelitian *online*
2. ***Hook*:** Penyerang mulai berinteraksi dengan target untuk membangun kepercayaan. Ini bisa melalui *email*, telepon, atau pertemuan tatap muka.
3. ***Play*:** Penyerang mengembangkan hubungan dengan target untuk mendapatkan lebih banyak informasi atau akses. Mereka mungkin menggunakan cerita palsu atau skenario yang meyakinkan untuk menipu target.

4. ***Exit*:** Penyerang mengeksploitasi informasi atau akses yang telah diperoleh untuk mencapai tujuan mereka, seperti mencuri data, uang, atau menyebabkan kerusakan pada sistem.



Video: https://www.youtube.com/watch?v=lc7scxvKQOo

Aspek yang terdampak oleh rekayasa sosial:

- **Fisik:** Rekayasa sosial dapat mengakibatkan akses fisik ke bangunan atau perangkat keras, misalnya melalui *tailgating* atau *baiting* dengan perangkat yang terinfeksi.
- **Sosial:** Penyerang dapat memanipulasi hubungan sosial untuk mendapatkan informasi, seperti berpura-pura menjadi teman atau kolega.
- **Psikososial:** Serangan ini dapat menimbulkan stres, ketakutan, atau rasa malu pada korban melalui ancaman atau pengungkapan informasi pribadi. Dampaknya bisa sangat merusak kesehatan mental dan emosional individu.

Kenapa ada rekayasa sosial?

Rekayasa sosial ada karena penyerang sering kali menemukan bahwa lebih mudah mengeksploitasi kelemahan manusia daripada mengatasi pertahanan teknis yang kuat. Manusia sering kali menjadi mata rantai terlemah dalam keamanan digital, sehingga mereka menjadi target utama untuk serangan semacam ini. Dengan memanfaatkan kepercayaan, ketakutan, atau kebiasaan manusia, penyerang dapat mencapai tujuan mereka tanpa harus menembus pertahanan teknologi yang kompleks.

Kapan terjadi rekayasa sosial?

Rekayasa sosial dapat terjadi kapan saja, terutama ketika seseorang tidak waspada atau dalam situasi yang rentan. Misalnya, serangan *phishing* sering kali terjadi saat jam kerja ketika karyawan sibuk dan mungkin kurang memperhatikan detail. Serangan lain, seperti *doxing*, bisa terjadi kapan saja, terutama ketika target berada dalam sorotan publik atau memiliki aktivitas *online* yang tinggi. Penyerang memanfaatkan momen-momen ketika korban paling tidak curiga atau paling rentan untuk mencapai tujuan mereka.

Tanda-tanda Rekayasa Sosial

Beberapa tanda yang perlu diwaspadai dalam serangan rekayasa sosial meliputi:

- Tautan atau logo yang mencurigakan.
- Bahasa yang aneh atau tata bahasa yang buruk.
- Pesan yang mengindikasikan urgensi atau ancaman.
- Komunikasi yang tidak terduga. Misalnya, *email phishing* sering kali meminta penerima untuk segera memasukkan informasi pribadi atau login ke situs palsu.

Langkah Pencegahan Rekayasa Sosial

Beberapa langkah pencegahan untuk menghindari rekayasa sosial meliputi:

- Membaca nama domain dengan hati-hati dan memeriksa keaslian tautan.
- Menghindari mengklik tautan atau lampiran yang mencurigakan.
- Mengunci perangkat dan menyimpan kata sandi dengan aman.
- Memeriksa *email* dengan teliti untuk menghindari *phishing* dan penipuan lainnya.

5

Asesmen Risiko dan Kesadaran Situasi

Asesmen & Manajemen Risiko

Manajemen risiko melibatkan proses identifikasi, analisa, mitigasi, dan pemantauan risiko yang dapat mempengaruhi kemampuan organisasi atau individu untuk mencapai tujuannya. Proses ini membantu dalam memahami dan merencanakan potensi risiko yang mungkin timbul.

Identifikasi Risiko

Identifikasi risiko adalah proses mendokumentasikan semua risiko yang dapat menghambat organisasi atau individu dalam mencapai tujuannya. Ini merupakan langkah pertama dalam manajemen risiko yang membantu kita memahami dan mempersiapkan diri terhadap potensi risiko. Identifikasi risiko memungkinkan kita untuk bersiap menghadapi peristiwa berbahaya dan meminimalkan dampaknya sebelum terjadi. Contohnya, seorang jurnalis yang bekerja di daerah konflik perlu mengidentifikasi risiko ancaman fisik dari pihak-pihak yang tidak setuju dengan liputannya.

Analisis Risiko

Analisis risiko dilakukan untuk menentukan penyebab utama masalah dan mengembangkan cara untuk

mengatasinya. Langkah-langkah yang bisa diambil meliputi:

- Menentukan masalah yang ada.
- Mengumpulkan data yang relevan.
- Menentukan faktor penyebab masalah.
- Mengidentifikasi akar penyebab masalah.

Sebagai contoh, ancaman terhadap aktivis yang berbicara tentang kekerasan berbasis gender dapat diidentifikasi dan dianalisis untuk menemukan cara-cara mengurangi risiko tersebut.

Manajemen/Mitigasi Risiko

Mengelola atau memitigasi risiko melibatkan beberapa langkah penting:

- Mengidentifikasi tindakan yang bisa dilakukan untuk memperbaiki masalah.
- Menemukan solusi yang dapat menghentikan masalah agar tidak terjadi lagi.
- Menjalankan solusi tersebut.
- Tindak lanjut untuk memastikan solusi berjalan efektif.

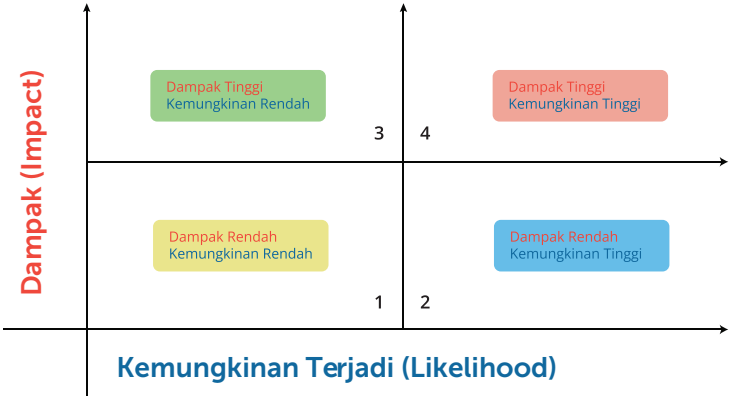
Contoh praktisnya adalah menggunakan analisis SWOT: ***Strengths*** (kekuatan), ***Weaknesses*** (kelemahan), ***Opportunities*** (peluang), dan ***Threats*** (ancaman) untuk mengidentifikasi kekuatan, kelemahan, peluang, dan ancaman dalam suatu proyek. Jika suatu daerah rawan bencana alam, rencana kegiatan bisa dipindahkan ke lokasi yang lebih aman.

Aktivitas Identifikasi Risiko

Langkah awal dalam manajemen risiko adalah mengidentifikasi risiko yang ada dan yang mungkin terjadi terkait dengan keamanan fisik, digital, dan kesejahteraan psikososial. Risiko ini dapat berkaitan dengan pekerjaan, keluarga, organisasi, kolega, dan

komunitas. Menuliskan sebanyak mungkin risiko yang teridentifikasi membantu dalam mengelola dan mengurangi dampak dari risiko tersebut.

Asesmen Risiko (Risk Assesment)



Asesmen Risiko

Menentukan Risiko yang Harus Diterima:

- Untuk risiko dengan dampak dan kemungkinan rendah (misalnya Risiko 1), sering kali lebih efisien untuk menerima risiko ini karena biaya untuk

menguranginya mungkin tidak sebanding dengan manfaatnya.

Menghindari Risiko:

- Menghindari risiko berarti mengambil tindakan untuk menghilangkan risiko sepenuhnya. Ini mungkin melibatkan perubahan rencana, prosedur, atau aktivitas yang dapat menyebabkan risiko tersebut. Contohnya, menghindari penggunaan teknologi tertentu yang diketahui rentan terhadap serangan siber.

Mentransfer Risiko:

- Mentransfer risiko berarti mengalihkan sebagian atau seluruh risiko kepada pihak ketiga, seperti melalui asuransi atau kontrak *outsourcing*. Contoh lain termasuk mengalihdayakan tugas yang berisiko tinggi kepada vendor yang memiliki keahlian khusus untuk menangani risiko tersebut.

Mengurangi Risiko:

- Mengurangi risiko melibatkan tindakan untuk mengurangi dampak atau kemungkinan terjadinya risiko. Ini bisa melibatkan implementasi kontrol keamanan tambahan, pelatihan karyawan, atau

peningkatan prosedur operasional. Contoh, meningkatkan keamanan digital dengan menerapkan autentikasi dua faktor untuk mengurangi risiko akses yang tidak sah.

Manajemen Risiko

Setelah identifikasi dan evaluasi risiko, mengikuti strategi sederhana dapat meminimalkan efek bahaya yang mungkin terjadi. Langkah-langkah ini meliputi:

- Memahami situasi yang terjadi.
- Memiliki rencana yang baik dan siap untuk menghadapi situasi tersebut.
- Menjalankan rencana yang telah disusun dan memantau pelaksanaannya.
- Membuat rencana cadangan untuk menghadapi skenario yang tidak terduga.

Aktivitas Membuat Rencana

Langkah ini melibatkan pemilihan masalah dari matriks penilaian risiko, membuat daftar kerentanan, mengidentifikasi tindakan untuk meminimalkan bahaya, menemukan solusi untuk mencegah terulangnya masalah, menjalankan solusi tersebut, dan membuat rencana cadangan.

Kesadaran Situasional *(Situational Awareness)*

Definisi Kesadaran Situasional

Kesadaran situasional adalah kemampuan untuk mengetahui apa yang terjadi di sekitar kita secara terus menerus. Ini melibatkan pengumpulan informasi dari lingkungan, integrasi informasi tersebut dengan pengetahuan sebelumnya untuk membentuk gambaran mengenai situasi dan konteks, dan penggunaan gambaran tersebut untuk mengarahkan persepsi lebih lanjut serta mengantisipasi kejadian di masa depan. Keadaan situasi sangat cair dan selalu berubah, oleh karena itu, individu harus tetap fleksibel dan terus mengamati serta menafsirkan lingkungan sekitar untuk membuat keputusan terbaik.

Empat A:
Ases, Analisa, Artikulasi, Aksi

Untuk mencapai kesadaran situasional yang optimal, kita dapat mengikuti pendekatan "Empat A":

1. **Ases Situasi:** Menilai apa yang ada di depan kita dan memahami konteks situasi.
2. **Analisa Informasi:** Menganalisis informasi yang telah dikumpulkan untuk menentukan apa yang penting dan apa yang perlu diprioritaskan.

3. **Artikulasi:** Membuat panggilan telepon, menulis di kertas, atau mengirim email untuk mendokumentasikan informasi dan rencana tindakan.
4. **Aksi:** Membuat keputusan berdasarkan asesmen dan analisa yang telah dilakukan, lalu mengambil tindakan yang sesuai.

Pemahaman

Pemahaman situasional melibatkan pemikiran kritis selama insiden terjadi. Individu harus terus-menerus mengidentifikasi pilihan, mempertimbangkan pro dan kontra dari setiap tindakan, dan membandingkan sebanyak mungkin variabel yang relevan.

Contohnya, dalam situasi darurat kebakaran, memahami di mana letak pintu keluar darurat dan jalur evakuasi sangat penting untuk keselamatan.

Kenali Lingkungan Sekitar Anda

Selalu mengetahui di mana kita berada, baik di dalam maupun di luar ruangan, sangat penting untuk keselamatan. Mengenali jalur untuk melarikan diri, tempat berlindung, dan potensi bahaya di sekitar dapat membantu kita bereaksi cepat dan tepat dalam situasi darurat.

Misalnya, di gedung perkantoran, mengetahui letak tangga darurat dan pintu keluar alternatif dapat menyelamatkan nyawa saat terjadi kebakaran.

Faktor yang Mempengaruhi Kesadaran Situasional

Beberapa faktor yang dapat mempengaruhi kesadaran situasional termasuk penglihatan terowongan *(tunnel vision),* tidak memindai secara keseluruhan, terlalu fokus atau keasyikan dengan satu hal, penggunaan *headphone*, bermain *handphone*, dan *chattingan*. Situasi yang dinamis memerlukan respon yang fleksibel, karena respon yang tidak fleksibel dapat menyebabkan kegagalan dalam mengatasi perubahan situasi.

6

Merawat Diri dan Perawatan Kolektif

Merawat diri adalah praktik melakukan hal-hal secara rutin dan teratur yang membuat Anda merasa lebih baik dengan cara yang aman dan berkelanjutan. Merawat diri melibatkan meluangkan waktu untuk melakukan aktivitas yang membantu Anda hidup dengan baik secara holistik, mencakup aspek fisik, mental, sosial, dan digital. Ini tidak hanya terbatas pada perawatan fisik seperti *skincare*, tetapi juga mencakup upaya menjaga kesejahteraan emosional dan psikologis.

Tujuan Merawat Diri

Tujuan merawat diri meliputi pemahaman konsep *self-care* dan manfaatnya, mengenali berbagai jenis *self-care,* serta membuat perencanaan *self-care* yang efektif. Dengan demikian, individu dapat menjaga keseimbangan hidup dan meningkatkan kesejahteraan mereka secara keseluruhan.

Mengapa Merawat Diri Perlu Dilakukan?

Merawat diri terbukti secara klinis dapat mengurangi kecemasan dan depresi, meningkatkan kekebalan tubuh, mengurangi stres, meningkatkan produktivitas, dan meningkatkan kesejahteraan mental, emosional, fisik, dan spiritual. Sebagai contoh, rutin berolahraga dapat membantu menjaga kebugaran fisik dan mengurangi

stres, sementara meditasi dapat meningkatkan kesejahteraan mental dan emosional.

Jenis-Jenis Merawat Diri

1. **Fisik**
    - **Aktivitas:** Berolahraga, tidur cukup dan teratur, cek kondisi medis berkala, makan makanan bergizi, serta memiliki asuransi kesehatan.
    - **Contoh:** Seorang aktivis yang rutin berolahraga dan menjaga pola makan yang sehat dapat menjaga kesehatan fisiknya dan meningkatkan energinya untuk melakukan pekerjaan advokasi.

2. **Emosional**
    - **Aktivitas:** Menulis jurnal, menangis, mempraktikkan teknik stabilisasi emosi, dan mendengarkan musik.
    - **Contoh:** Menulis jurnal dapat membantu seseorang dalam memproses emosi mereka dan menemukan cara untuk mengatasi stres.

3. **Psikologis**
    - **Aktivitas:** Mengembangkan minat dan hobi, refleksi diri, menerima bantuan, belajar hal baru, *detox digita*l, dan mengakses layanan kesehatan mental.
    - **Contoh:** Mengikuti kelas memasak sebagai hobi baru dapat memberikan rasa pencapaian dan kebahagiaan, serta menjadi sarana untuk mengalihkan pikiran dari tekanan pekerjaan.

4. **Profesional**
    - **Aktivitas:** Menetapkan target kerja yang realistis, manajemen waktu, membangun batasan *(boundaries),* memantau paparan konten traumatis, memberikan jeda antara tugas, mengikuti *debriefing,* dan membangun hubungan positif dengan rekan kerja.
    - **Contoh:** Seorang pekerja sosial yang menetapkan batasan waktu kerja yang jelas dapat menghindari *burnout* dan menjaga keseimbangan antara kehidupan kerja dan pribadi.

5. **Sosial**
    - **Aktivitas:** Bertemu dengan teman-teman, mengikuti komunitas, menjadi sukarelawan, dan menghabiskan waktu dengan pasangan serta keluarga.
    - **Contoh:** Bergabung dengan komunitas hobi dapat memberikan dukungan sosial yang kuat dan meningkatkan kesejahteraan emosional.

6. **Spiritual**
    - **Aktivitas:** Beribadah, berdoa, berjalan-jalan di alam, meditasi, mengikuti kajian agama, dan refleksi diri.
    - **Contoh:** Meditasi secara teratur dapat membantu menenangkan pikiran dan memberikan kedamaian batin.

Hambatan dalam Melakukan Merawat diri

Beberapa hambatan umum dalam melakukan *self-care* meliputi keinginan untuk melakukan semuanya sekaligus, merasa bersalah, ekspektasi yang tidak realistis, aktivitas *self-care* yang tidak sesuai dengan kebutuhan,

dan kurangnya dukungan dari lingkungan. Misalnya, seorang aktivis mungkin merasa bersalah meluangkan waktu untuk diri sendiri karena merasa harus selalu siap membantu orang lain.

Membangun Batasan (*Boundaries*)

Batasan pribadi adalah batasan fisik, emosional, dan mental yang digunakan seseorang untuk melindungi diri agar tidak terlalu terlibat dalam kehidupan kliennya dan agar tidak dimanipulasi atau dilanggar oleh orang lain. Misalnya, seorang pekerja sosial yang menetapkan batasan yang jelas tentang jam kerja dapat menghindari kelelahan dan menjaga keseimbangan kehidupan kerja.

Latihan untuk Mengatakan "Tidak"

Mengatakan "tidak" pada suatu permintaan mungkin terasa tidak nyaman, namun dengan latihan hal itu akan menjadi lebih mudah. Semakin baik Anda mengatakan "tidak", semakin besar pula kemampuan Anda untuk mengatakan "ya" terhadap prioritas Anda. Misalnya, ketika teman meminta untuk meminjam mobil Anda dan Anda merasa tidak nyaman, Anda bisa menolak dengan sopan dan menawarkan alternatif lain.

Definisi Perawatan Kolektif

Perawatan kolektif adalah pendekatan di mana komunitas atau kelompok bersama-sama bertanggung jawab untuk memastikan kesejahteraan dan keamanan anggotanya. Ini melibatkan dukungan dan perhatian bersama untuk menciptakan lingkungan yang saling mendukung, di mana setiap anggota merasa dilindungi dan dihargai. Contoh dari perawatan kolektif adalah ketika anggota sebuah komunitas saling membantu dalam situasi krisis, seperti memberikan dukungan emosional, berbagi sumber daya, dan menjaga satu sama lain dari bahaya.

Manfaat Perawatan Kolektif

Manfaat utama dari perawatan kolektif meliputi peningkatan kesejahteraan emosional dan psikologis, pengurangan stres, dan peningkatan rasa solidaritas dan kohesi sosial di antara anggota komunitas. **Ketika individu merasa didukung oleh komunitas mereka, mereka cenderung lebih resilien dalam menghadapi tantangan dan krisis.** Misalnya, dalam kelompok dukungan untuk korban kekerasan berbasis gender, anggota kelompok saling memberikan dukungan emosional dan praktis yang membantu mereka pulih dan merasa lebih aman.

Strategi Perawatan Kolektif

1. **Dukungan Emosional:** Menciptakan ruang aman di mana anggota komunitas dapat berbagi perasaan dan pengalaman mereka tanpa takut akan penilaian atau stigma. Misalnya, mengadakan sesi kelompok untuk berbagi cerita dan mendiskusikan strategi *coping* dapat membantu mengurangi beban emosional

2. **Berbagi Sumber Daya:** Memastikan bahwa semua anggota komunitas memiliki akses ke sumber daya yang mereka butuhkan, seperti makanan, tempat tinggal, dan layanan kesehatan. Ini dapat mencakup pengumpulan dana bersama, berbagi makanan, atau menyediakan transportasi bagi mereka yang membutuhkan.

3. **Pendidikan dan Pelatihan:** Menyediakan pendidikan dan pelatihan tentang pentingnya *self-care* dan bagaimana menerapkannya dalam kehidupan sehari-hari. Misalnya, mengadakan lokakarya tentang manajemen stres, teknik relaksasi, dan keterampilan hidup yang sehat.

4. **Komunikasi Terbuka:** Memastikan bahwa ada saluran komunikasi yang terbuka dan transparan antara anggota komunitas. Ini membantu mencegah kesalahpahaman dan memastikan bahwa setiap orang merasa didengar dan dihargai. Contohnya, menggunakan *platform* komunikasi *online* untuk diskusi kelompok dan pembaruan berita komunitas.

5. **Pengambilan Keputusan Kolektif:** Melibatkan semua anggota komunitas dalam proses pengambilan keputusan untuk memastikan bahwa setiap suara didengar dan dihargai. Ini dapat dilakukan melalui pertemuan komunitas reguler, survei, atau sistem *voting*.

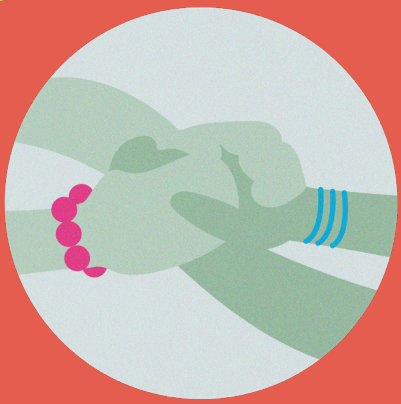
Contoh Perawatan Kolektif dalam Praktek

- **Komunitas Aktivis:** Aktivis yang bekerja di daerah berisiko tinggi sering kali mengembangkan jaringan dukungan kolektif untuk memastikan keamanan mereka. Ini dapat mencakup rotasi penjagaan, berbagi informasi intelijen, dan menyediakan tempat tinggal aman bagi anggota yang menghadapi ancaman langsung.

- **Program Dukungan di Tempat Kerja:** Beberapa organisasi menyediakan program dukungan karyawan yang mencakup konseling, kelompok dukungan, dan pelatihan manajemen stres untuk membantu karyawan mengatasi tekanan kerja dan menjaga kesejahteraan mereka.
- **Kelompok Dukungan Masyarakat:** Kelompok dukungan masyarakat untuk individu yang mengalami penyakit kronis atau kondisi kesehatan mental menyediakan ruang bagi anggota untuk berbagi pengalaman mereka, memberikan dukungan emosional, dan berbagi strategi untuk mengelola kondisi mereka.

Dengan menerapkan strategi perawatan kolektif, komunitas dapat menciptakan lingkungan yang lebih aman dan mendukung, di mana setiap individu merasa dihargai dan terlindungi. Pendekatan ini tidak hanya meningkatkan kesejahteraan individu tetapi juga memperkuat solidaritas dan kohesi sosial di antara anggota komunitas.


Apa Kabar?
Baik. kamu?
Aku juga kabar baik..



7

Pertolongan Dasar Holistik

Apa Itu Pertolongan Pertama Psikologis?

Pertolongan pertama psikologis *(Psychological First Aid* atau *PFA)* adalah pendekatan berbasis bukti yang digunakan untuk membantu individu segera setelah terjadinya bencana, krisis, atau peristiwa traumatis. Tujuannya adalah untuk mengurangi tekanan awal, mendorong fungsi adaptif jangka pendek dan panjang, serta mendukung kesehatan mental dan kesejahteraan.

PFA dirancang agar sederhana dan praktis, memungkinkan baik profesional maupun non-profesional untuk memberikan dukungan. Contohnya, seorang relawan yang memberikan dukungan emosional kepada korban bencana alam dengan cara mendengarkan dengan empati dan memberikan informasi yang menenangkan. **Untuk bahan bacaan lebih lanjut silahkan buka tautan berikut:**

https://www.perempuanberkisah.id/2022/07/26/psychological-first-aid-pfa-pada-korban-kekerasan-seksual/

Prinsip Utama Pertolongan Pertama Psikologis

1. **Keamanan dan Kenyamanan:** Memastikan bahwa individu merasa aman dan nyaman setelah mengalami peristiwa traumatis. Misalnya,

menyediakan lingkungan yang tenang dan aman untuk berbicara.

2. **Stabilisasi:** Membantu individu menstabilkan emosi mereka untuk mencegah kondisi menjadi lebih buruk. Ini bisa dilakukan dengan teknik pernapasan atau berbicara secara tenang.

3. **Menghubungkan dengan Sistem Pendukung:** Membantu individu terhubung kembali dengan keluarga, teman, atau layanan dukungan lainnya. Misalnya, memberikan informasi kontak untuk layanan kesehatan mental.

4. **Bantuan Praktis:** Memberikan bantuan praktis seperti makanan, tempat tinggal, atau informasi penting.

5. **Mengumpulkan Informasi Terkait Kebutuhan:** Mengidentifikasi kebutuhan spesifik individu untuk memberikan bantuan yang sesuai.

6. **Menghubungkan dengan Tenaga Layanan:** Mengarahkan individu kepada profesional yang dapat memberikan bantuan lebih lanjut jika diperlukan.

Memberikan Kenyamanan dan Informasi

Untuk memberikan kenyamanan, **penting untuk mendengarkan dengan empati dan melindungi individu dari situasi yang dapat memperburuk kondisi mereka.** Selain itu, memberikan informasi yang akurat dan mendukung mereka dalam mengambil keputusan penting dapat membantu mereka merasa lebih terkendali dan tenang. Misalnya, saat menghadapi korban bencana, mendengarkan kisah mereka tanpa menghakimi dan memberikan informasi tentang langkah-langkah berikutnya dalam proses pemulihan.

Prinsip PFA 3L: *Look, Listen, and Link*

Video: https://www.youtube.com/watch?v=kly45u9ml_A

Pertolongan Pertama Psikologis *(Psychological First Aid* atau *PFA)* adalah pendekatan berbasis bukti yang digunakan untuk membantu individu setelah terjadinya

bencana, krisis, atau peristiwa traumatis. Prinsip utama PFA adalah *"Look, Listen, and Link,"* yang memberikan panduan bagi pemberi bantuan untuk mendukung korban secara efektif dan empatik.

Look (Melihat)

Langkah pertama dalam PFA adalah mengamati situasi dan memahami kebutuhan langsung korban. Ini melibatkan:

1. **Mengamati Lingkungan:** Menilai keselamatan lingkungan sekitar untuk memastikan bahwa tidak ada bahaya langsung yang mengancam korban dan pemberi bantuan. Misalnya, jika terjadi bencana alam, pastikan bahwa area tersebut aman dari reruntuhan atau potensi bahaya lainnya sebelum memberikan bantuan.

2. **Mengenali Tanda-Tanda Distres:** Mengidentifikasi individu yang menunjukkan tanda-tanda distres atau trauma, seperti terlihat bingung, cemas, menangis, atau terdiam. Amati perilaku fisik dan emosional mereka untuk memahami tingkat keparahan stres yang mereka alami.

3. **Menentukan Prioritas Bantuan:** Menilai siapa yang membutuhkan bantuan segera berdasarkan kondisi fisik dan emosional mereka. Misalnya, seseorang yang terluka parah atau sangat cemas mungkin memerlukan bantuan lebih cepat daripada yang lainnya.

Listen (Mendengarkan)

Langkah kedua adalah mendengarkan korban dengan penuh perhatian dan empati. Ini melibatkan:

1. **Menyediakan Ruang Aman:** Ciptakan lingkungan di mana korban merasa aman untuk berbicara tanpa takut dihakimi atau diinterupsi. Pastikan bahwa tempat tersebut cukup tenang dan privat untuk mendiskusikan perasaan mereka.

2. **Mendengarkan Aktif:** Dengarkan dengan penuh perhatian tanpa menghakimi. Gunakan bahasa tubuh yang terbuka, seperti menganggukkan kepala, mempertahankan kontak mata, dan memberikan respons verbal singkat seperti “Saya mengerti” atau “Itu pasti sulit.”

3. **Mengajukan Pertanyaan Terbuka:** Ajukan pertanyaan yang memungkinkan korban untuk

menceritakan pengalaman mereka secara lebih rinci, seperti “Bagaimana perasaan Anda saat ini?” atau “Bisakah Anda ceritakan apa yang terjadi?” Hindari pertanyaan yang terlalu mengarahkan atau menghakimi.

Link (Menghubungkan)

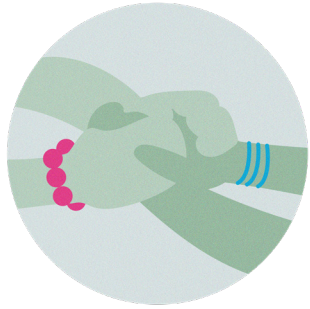
Langkah ketiga adalah menghubungkan korban dengan layanan dukungan dan sumber daya yang mereka butuhkan. Ini melibatkan:

1. **Memberikan Informasi Praktis:** Berikan informasi tentang layanan dan dukungan yang tersedia, seperti tempat penampungan sementara, layanan medis, atau bantuan psikologis. Pastikan informasi tersebut mudah dipahami dan dapat diakses oleh korban.

2. **Menghubungkan dengan Jaringan Dukungan:** Bantu korban terhubung dengan keluarga, teman, atau jaringan dukungan lain yang dapat memberikan bantuan tambahan. Ini dapat melibatkan menghubungi anggota keluarga atau teman terdekat mereka

3. **Mengikuti Protokol Layanan:** Pandu korban melalui langkah-langkah untuk mengakses

layanan yang diperlukan, seperti cara mendaftar untuk bantuan keuangan, menghubungi layanan kesehatan mental, atau mendapatkan dukungan hukum. Misalnya, memberikan nomor telepon atau alamat email layanan dukungan yang relevan dan membantu mereka menghubungi layanan tersebut.



Pertolongan Pertama Holistik Saat Menghadapi Risiko Fisik

Penggerebekan Kantor

Saat menghadapi penggerebekan kantor, langkah pertama yang harus dilakukan adalah tetap tenang dan fokus (gunakan Teknik pernapasan dan *grounding)*. Hindari panik karena hanya akan memperburuk situasi. Prioritaskan keselamatan diri dan rekan kerja dengan mengikuti instruksi dari pemimpin tim atau petugas keamanan. Penting untuk mengetahui rute evakuasi yang aman sebelum terjadi penggerebekan. Pastikan semua karyawan mengetahui letak pintu darurat dan rute evakuasi yang telah ditetapkan. Gunakan pintu darurat dan hindari pintu utama jika tidak aman. Bekerja berpasangan atau menggunakan sistem *buddy* dapat memastikan tidak ada yang tertinggal atau terluka. Sebelum meninggalkan gedung, periksa kehadiran semua anggota tim untuk memastikan semua sudah dievakuasi. Selain itu, segera hubungi lembaga bantuan hukum dan dokumentasikan kejadian untuk keperluan investigasi dan laporan jika situasi memungkinkan.

Kegiatan yang Berisiko

Dalam kegiatan yang berisiko, persiapan awal sangat penting. Lakukan penilaian risiko sebelum kegiatan dimulai untuk mengidentifikasi potensi bahaya dan merencanakan tindakan pencegahan. Bawa peralatan pertolongan pertama, air minum, makanan ringan, dan alat komunikasi. Selama kegiatan, terus pantau situasi di sekitar dan cari informasi dari sumber yang dapat dipercaya. Jauhi area yang menunjukkan tanda-tanda bahaya atau ketidakstabilan. Koordinasi dengan tim atau kelompok Anda sangat penting untuk memastikan keselamatan bersama. Tentukan tanda-tanda darurat untuk berkomunikasi jika terjadi situasi berbahaya.

Aksi Protes yang Berubah Rusuh

Jika terjadi aksi protes yang berubah menjadi rusuh, segera jauhi area terdampak. Jika gas air mata mulai digunakan, segera menjauh dari area tersebut melawan arah angin dan cari tempat yang aman. Lindungi mata dan saluran pernapasan dengan menggunakan kacamata pelindung dan kain basah atau masker untuk menutupi hidung dan mulut. Tetap berkoordinasi dengan korlap dan tim bantuan hukum. Jika memungkinkan, dokumentasikan kejadian untuk keperluan laporan dan bukti. Setelah terkena gas air mata, bilas mata dengan air

bersih atau larutan garam dan hindari menggosok mata untuk mencegah iritasi lebih lanjut. Segera ganti pakaian yang terkena gas air mata untuk menghindari iritasi kulit. Cari tempat aman untuk beristirahat dan mengatur napas, dan hindari area tertutup yang tidak memiliki ventilasi baik.

Kesimpulan

Menghadapi risiko fisik memerlukan persiapan dan tindakan cepat untuk memastikan keselamatan diri dan orang lain. Dengan mengikuti panduan pertolongan pertama holistik yang mencakup aspek fisik, psikososial, dan digital, individu dan kelompok dapat lebih siap menghadapi situasi darurat dan memastikan kesejahteraan semua

pihak yang terlibat. Misalnya, dalam penggerebekan kantor, tetap tenang dan fokus, gunakan sistem *buddy*, dan hubungi lembaga bantuan hukum. Dalam kegiatan berisiko, lakukan penilaian risiko, bawa peralatan darurat, dan pantau situasi. Dalam aksi rusuh, jauhi area terdampak, lindungi diri, dan dokumentasikan kejadian jika memungkinkan.

Pertolongan Pertama Keamanan Digital

1. **Deteksi dan Respons Awal**

   Langkah pertama dalam menangani insiden keamanan digital adalah mendeteksi dan merespons dengan cepat. Jika Anda mencurigai bahwa perangkat atau akun Anda telah dikompromikan, penting untuk bertindak segera untuk mengurangi kerusakan. Misalnya, jika Anda melihat aktivitas mencurigakan seperti *login* dari lokasi yang tidak dikenal, segera *log out* dari semua sesi aktif dan ubah kata sandi Anda.

2. **Ganti Kata Sandi dan Autentikasi Dua Faktor (2FA)**

   Segera ganti kata sandi semua akun yang mungkin terpengaruh. Pastikan kata sandi baru kuat dan unik, berbeda dari kata sandi yang digunakan sebelumnya. Selain itu, aktifkan autentikasi dua faktor (2FA) pada semua akun yang mendukung fitur ini. 2FA menambahkan lapisan keamanan ekstra dengan mengharuskan verifikasi identitas melalui perangkat lain selain kata sandi.

3. **Cek dan Hapus Perangkat yang Tidak Dikenal**

   Periksa daftar perangkat yang terhubung ke akun Anda. Jika Anda menemukan perangkat yang tidak dikenali atau tidak dikenal, segera hapus aksesnya. Misalnya, layanan seperti *Google* dan *Facebook* memungkinkan Anda untuk melihat dan mengelola perangkat yang telah mengakses akun Anda.

4. **Perbarui Perangkat Lunak dan Sistem Keamanan**

   Pastikan semua perangkat lunak, aplikasi, dan sistem operasi Anda diperbarui dengan *patch* keamanan terbaru. Pembaruan ini sering kali mencakup perbaikan untuk kerentanan yang telah diketahui. Menggunakan versi perangkat lunak terbaru dapat mencegah penyerang mengeksploitasi celah keamanan yang sudah diperbaiki.

5. **Pindai dan Bersihkan Perangkat dari *Malware***

   Jalankan pemindaian antivirus dan *antimalware* pada semua perangkat untuk mendeteksi dan menghapus program jahat. Alat seperti

Malwarebytes atau *Windows Defender* dapat membantu dalam mendeteksi dan menghapus malware yang mungkin telah menginfeksi perangkat Anda.

6. **Lakukan *Backup* Data**

   Segera lakukan *backup* data penting ke lokasi yang aman, seperti hard drive eksternal atau layanan *cloud* yang tepercaya. *Backup* data memastikan bahwa Anda memiliki salinan cadangan jika data utama Anda terhapus atau dikompromikan. Pastikan *backup* terenkripsi untuk melindungi data dari akses yang tidak sah.

7. **Cek Aktivitas Akun dan Keamanan**

   Periksa aktivitas terbaru pada semua akun Anda untuk mendeteksi aktivitas yang tidak sah. Beberapa layanan, seperti *Google* dan *Facebook,* memiliki fitur untuk melihat log aktivitas yang mencurigakan. Jika menemukan aktivitas yang tidak dikenali, laporkan kepada penyedia layanan dan ikuti petunjuk mereka untuk mengamankan akun.

8. **Edukasi Diri tentang *Phising* dan Teknik Rekayasa Sosial**

   Phishing adalah salah satu metode paling umum yang digunakan untuk mencuri informasi pribadi. Pelajari cara mengenali email, pesan teks, atau situs web *phishing* dan hindari mengklik tautan atau lampiran yang mencurigakan. Selalu verifikasi sumber komunikasi sebelum memberikan informasi pribadi atau sensitif.

9. **Gunakan Alat Keamanan Digital**

   Manfaatkan alat dan layanan yang tersedia untuk meningkatkan keamanan digital Anda. Beberapa alat yang bermanfaat meliputi:

   - **Last Pass** untuk membuat dan menyimpan kata sandi yang kuat.
   - **Virus Total** dan **URL Scan** untuk memeriksa keamanan tautan dan file yang mencurigakan.
   - **Have I Been Pawned** untuk memeriksa apakah email atau kata sandi Anda telah bocor.
   - **Google Security Checkup** untuk memeriksa pengaturan keamanan akun Google Anda.

Lapor dan Dapatkan Bantuan

Jika Anda merasa bahwa data atau akun Anda telah disusupi, segera laporkan insiden tersebut ke penyedia layanan dan ikuti petunjuk mereka. Anda juga bisa melaporkan pelanggaran hak digital atau kekerasan berbasis gender *online* ke layanan seperti SAFEnet atau *platform* lainnya yang relevan. Mereka dapat memberikan dukungan dan panduan lebih lanjut untuk mengatasi situasi tersebut.

Contoh Kasus dan Implementasi

Misalnya, seorang aktivis hak asasi manusia yang melihat aktivitas mencurigakan di akun *email*nya segera mengganti kata sandi dan mengaktifkan 2FA. Dia juga memindai laptopnya dengan perangkat lunak *antimalware* dan melakukan *backup data* penting ke layanan *cloud* yang terenkripsi. Aktivis tersebut kemudian melaporkan insiden tersebut ke penyedia layanan *email* dan mengikuti panduan mereka untuk mengamankan akun.

Dengan mengikuti langkah-langkah di atas, individu dan organisasi dapat meningkatkan keamanan digital mereka dan mengurangi risiko yang terkait dengan insiden keamanan digital.


Apa Kabar?
Baik. kamu?
Aku juga kabar baik..

Komunikasi Aman

Komunikasi aman adalah praktik yang penting untuk melindungi privasi dan keamanan informasi pribadi, terutama dalam konteks kekerasan berbasis gender *online* (KBGO) dan ancaman digital lainnya. Materi ini memberikan panduan tentang cara berkomunikasi dengan aman menggunakan berbagai perangkat dan aplikasi, serta bagaimana mengelola keamanan dan privasi secara efektif.

Ditujukan untuk Apa dan Siapa?

Komunikasi aman ditujukan untuk siapa saja yang ingin melindungi informasi pribadi mereka dari akses yang tidak sah. Ini melibatkan berbagai pihak, termasuk individu yang sering berkomunikasi *online*, organisasi yang menangani data sensitif, serta komunitas yang rentan terhadap ancaman digital. Misalnya, seorang aktivis HAM yang bekerja di lingkungan berisiko tinggi perlu memahami bagaimana melindungi komunikasi mereka dari pihak-pihak yang berusaha mengganggu atau menyabotase upaya mereka.

Perangkat dan Aplikasi yang Digunakan

Komunikasi aman memerlukan perangkat dan aplikasi yang mendukung pengaturan keamanan dan privasi yang kuat. Pengguna harus memastikan bahwa perangkat

mereka dilengkapi dengan enkripsi, autentikasi dua faktor (2FA), dan pengaturan privasi yang tepat. Misalnya, menggunakan aplikasi pesan terenkripsi seperti *Signal* atau *WhatsApp* dengan 2FA diaktifkan dapat meningkatkan keamanan komunikasi.

Aksesibilitas dan Keamanan Aplikasi

Penting untuk mempertimbangkan siapa saja yang dapat mengakses perangkat dan aplikasi yang digunakan. Pengguna harus memastikan bahwa hanya orang-orang terpercaya yang memiliki akses ke informasi sensitif. Selain itu, pengguna harus selalu mengupdate perangkat lunak dan mengelola izin aplikasi untuk mengurangi risiko akses yang tidak sah.

Kapan dan Dimana Komunikasi Dilakukan

Komunikasi aman juga harus mempertimbangkan waktu dan tempat komunikasi dilakukan. Misalnya, saat melakukan komunikasi penting, hindari melakukannya di ruang publik yang diawasi CCTV atau saat menggunakan jaringan *Wi-Fi* publik yang tidak aman. Memastikan bahwa komunikasi tidak bisa di-*copy* atau di-*screenshot* juga penting untuk melindungi informasi sensitif.

Kebijakan dan Manajemen Komunikasi

Mengembangkan kebijakan terkait manajemen komunikasi, privasi, data, perangkat, dan manusia adalah langkah penting untuk memastikan keamanan kolektif. Ini termasuk kebijakan penggunaan perangkat, pengelolaan data pribadi, dan prosedur darurat jika terjadi pelanggaran keamanan. Misalnya, sebuah organisasi harus memiliki kebijakan yang mengatur penggunaan perangkat kerja untuk memastikan bahwa data sensitif tidak disimpan atau diakses dari perangkat pribadi yang tidak aman.

Reka

follow

0 posts 2000 followers 1000 following

“Risiko Tidak Bisa Dihilangkan, Selalu Bisa Dikurangi”

This Account is Private

9

Mekanisme Penanganan dan Rujukan Laporan

Prinsip Keamanan Digital

Beberapa prinsip keamanan digital yang harus diikuti meliputi:

1. **Saling Terkait:** Semakin memudahkan kita, semakin memudahkan pihak lain. Satu lalai, semua terancam. Keamanan harus dipahami sebagai tanggung jawab bersama.

2. **Kebiasaan Rutin:** Jadikan keamanan digital sebagai kebiasaan rutin. Lakukan pengecekan jejak digital, penyesuaian pengaturan, diversifikasi aset, *backup* sesuai kebutuhan, serta inventarisasi dan pemindaian secara berkala.

3. **Aspek Psikososial:** Perhatikan aspek psikososial, baik *offline* (fisik) maupun *online* (digital). Pertimbangkan dampak personal dan kolektif, serta perbedaan antara privasi dan publik.

4. ***Update & Upgrade:*** Selalu *update* dan *upgrade hardware, software*, dan *brainware* untuk memastikan bahwa semua perangkat dan sistem tetap aman.

5. **Enkripsi:** Gunakan enkripsi untuk melindungi perangkat, data, dan komunikasi. Pastikan semua

data yang disimpan dan dikirim terlindungi dengan baik.

Risiko Tidak Bisa Dihilangkan, Selalu Bisa Dikurangi

Meskipun risiko keamanan digital tidak bisa dihilangkan sepenuhnya, selalu ada cara untuk menguranginya. Beberapa alat bantu yang dapat digunakan untuk meningkatkan keamanan meliputi:

- **Kekuatan Kata Sandi:** Menggunakan layanan seperti *LastPass* untuk memastikan kata sandi yang kuat.
- **URL/File Mencurigakan:** Menggunakan *VirusTotal* atau *URLScan* untuk memeriksa keamanan tautan atau file.
- **Kebersihan Digital:** Mengikuti panduan *Data Detox Kit* untuk membersihkan jejak digital.
- **Cek Kebocoran Data:** Menggunakan *Have I Been Pawned* untuk memeriksa apakah data Anda telah bocor.
- **Cek Pengaturan Google:** Melakukan pemeriksaan keamanan dan privasi di *Google.*
- **Autentikasi 2-Faktor:** Mengaktifkan 2FA melalui *platform* seperti Internet Sehat atau *Two Factor Authentication*.

Kanal Laporan dan Pengada Layanan

Jika terjadi pelanggaran hak digital atau kekerasan berbasis gender *online*, penting untuk mengetahui kanal laporan yang tersedia. SAFEnet menyediakan layanan aduan untuk pelanggaran hak digital dan kekerasan berbasis gender *online.* Pengguna juga bisa melaporkan hoaks melalui Mafindo atau Kemenkominfo, serta mengakses rujukan dari Komnas Perempuan dan KemenPPPA untuk kekerasan terhadap perempuan.

Dengan memahami dan menerapkan prinsip-prinsip komunikasi aman ini, individu dan organisasi dapat melindungi informasi pribadi mereka dan mengurangi risiko ancaman digital. Pendekatan ini tidak hanya membantu menjaga privasi tetapi juga memastikan bahwa komunikasi dapat dilakukan dengan aman dan efektif.

Mekanisme Penanganan dan Rujukan Kasus

Tahap Persiapan

Tentukan layanan yang sesuai dengan visi dan misi Lembaga.

Pastikan setiap layanan atau respon selaras dengan nilai-nilai, visi, dan misi organisasi. Evaluasi mendalam

diperlukan untuk memastikan aktivitas mendukung tujuan jangka panjang. Misalnya, jika Lembaga fokus pada pemberdayaan perempuan dan anak, layanan harus meningkatkan kualitas hidup dan melindungi hak-hak mereka. Layanan yang tepat menjaga konsistensi dan integritas operasional Lembaga.

Ukur kapasitas dan sumber daya yang ada di Lembaga.

Evaluasi kapasitas dan sumber daya sebelum memutuskan layanan. Ini mencakup sumber daya manusia, waktu, tenaga, dan ekonomi untuk biaya tak terduga. Pastikan Lembaga mampu memberikan layanan tanpa membebani tim atau anggaran. Tinjau juga apakah sudah ada Standar Operasional Prosedur (SOP) yang relevan untuk mendukung layanan. SOP yang jelas membantu pengelolaan sumber daya dan pelaksanaan layanan efisien.

Lakukan asesmen terhadap risiko dan ancaman yang mungkin dihadapi.

Asesmen risiko diperlukan untuk mengidentifikasi potensi masalah dalam menyediakan atau menambah layanan. Risiko bisa berupa ancaman keamanan, kerentanan terhadap serangan siber, atau kendala

finansial. Dengan memahami risiko ini, Lembaga dapat menyiapkan strategi mitigasi yang efektif untuk mengurangi dampak negatif dan memastikan kelancaran operasional.

Buatlah sistem kerja yang jelas yang diketahui semua anggota Lembaga.

Miliki sistem kerja yang terstruktur dan terdokumentasi dengan baik yang diketahui semua anggota Lembaga. Sistem harus mencakup proses penanganan laporan, tindakan yang akan diambil, jenis layanan yang diberikan, dan sejauh mana layanan berjalan. Dokumentasi yang jelas memastikan semua anggota memahami peran dan tanggung jawab mereka serta prosedur yang harus diikuti. Hal ini meningkatkan efisiensi operasional dan memastikan layanan konsisten sesuai standar Lembaga.

Target penerima

Tentukan target penerima: Tentukan dengan jelas siapa yang akan menjadi target dari layanan yang akan diberikan. Contoh diantaranya:

- Aktivis
- Organisasi non-pemerintah

- Pembela hak asasi manusia
- Organisasi hak asasi manusia yang berisiko
- Media independen
- Organisasi masyarakat adat
- Jurnalis
- Pembela lingkungan
- Kelompok LGBTQIA+
- Perempuan
- Pemuda (rentang usia tertentu)
- Lainnya

Menerima Laporan/Aduan

Identifikasi saluran komunikasi terbaik bagi penerima manfaat Anda untuk mendapatkan dukungan dari saluran bantuan atau meja bantuan. Berdasarkan analisis konteks awal dan model ancaman, pertimbangkan apakah penerima manfaat Anda membutuhkan enkripsi *end-to-end* atau mekanisme pengambilan data anonim sejak awal. Jika ini kasusnya, pikirkan semua metode yang memungkinkan untuk bertukar informasi sensitif melalui saluran yang aman.

Kami merekomendasikan untuk menyediakan setidaknya dua cara berbeda untuk menghubungi meja bantuan Anda:

- Saluran yang dapat diakses oleh semua orang tanpa pengetahuan teknis, seperti alamat email.
- Saluran yang aman bagi orang-orang yang memiliki pengetahuan teknis yang diperlukan untuk menggunakannya, seperti email terenkripsi atau aplikasi pesan aman seperti *Signal* atau *Wire.*

Menjamin keamanan komunikasi sangat penting. Namun, prioritas Anda adalah memastikan bahwa pelapor Anda mudah dijangkau. Oleh karena itu, penting untuk menawarkan beberapa saluran komunikasi bagi penerima manfaat Anda. Memperbanyak saluran komunikasi tidak selalu menjadi masalah selama tim Anda terorganisir dengan baik untuk berbagi informasi.

Berikut adalah daftar alat komunikasi yang dapat ditawarkan kepada penerima manfaat mereka sebagai metode yang mungkin untuk menjalin kontak pertama dengan organisasi tempat mereka melapor:

- Formulir web anonim
- *Email*
- *Email* terenkripsi PGP
- Telepon
- Surat pos
- *Signal*
- *Skype*
- *Telegram*
- Formulir web
- *WhatsApp*
- *Wire*

Pertimbangkan juga bahwa beberapa penerima manfaat Anda mungkin telah mengalami peristiwa traumatis dan mungkin membutuhkan mendengarkan aktif dan empati, yang paling baik dicapai melalui panggilan telepon atau video.

Ada juga banyak pilihan untuk mempertahankan hubungan dengan penerima manfaat dan menerima umpan balik, termasuk:

- Forum
- Grup bersama
- Pertemuan, konferensi, lokakarya, presentasi (tatap muka dan jarak jauh)
- Media sosial

Menyatakan Ketersediaan dan Waktu Respon Anda

Anda harus mengkomunikasikan waktu respon Anda dengan jelas kepada penerima manfaat untuk menghindari ekspektasi yang salah dan untuk menetapkan perjanjian mengenai layanan yang anda berikan. **Memberikan respon tepat waktu kepada penerima manfaat selama penanganan insiden sangat penting, baik untuk menangani masalah yang mereka hadapi maupun untuk reputasi organisasi anda.**

Ketersediaan dan waktu respon akan sangat bergantung pada jumlah anggota staf Anda dan jam kerja mereka. Kecuali organisasi mau menyediakan layanan 24/7, Anda perlu memutuskan bagaimana insiden dapat dilaporkan di luar jam kerja. Anda bisa memilih untuk memeriksa semua pesan masuk pada hari kerja berikutnya, atau Anda bisa memiliki anggota tim yang bertugas untuk memantau permintaan yang masuk dan memutuskan urgensinya.

Penting untuk mempertimbangkan konteks Anda saat membuat keputusan ini: misalnya, **jika Anda memiliki pendanaan terbatas, Anda mungkin tidak mampu membayar operator untuk bekerja di luar jam kerja standar. Ini juga merupakan pertimbangan penting**

untuk keamanan psikososial staf Anda: jika, misalnya, organisasi Anda dioperasikan oleh relawan, mereka mungkin bersedia menerima permintaan pada setiap jam siang atau malam, tetapi ini bisa dengan cepat menyebabkan kelelahan pada operator yang paling berdedikasi.

Menentukan Jenis Layanan yang akan diberikan dan Batasan

Organisasi dapat menawarkan berbagai layanan, tetapi selama Anda menyediakan beberapa jenis respon insiden, **Anda tidak perlu melakukan semuanya dan dapat fokus pada sejumlah layanan inti.** Misalnya, Anda bisa fokus pada keamanan akun media sosial atau memberikan rekomendasi tentang cara menghindari sensor di area tertentu, memberikan edukasi terhadap keamanan kantor dan keamanan fisik lainnya, atau memberikan pendampingan psikososial bagi korban kekerasan seksual.

Organisasi juga bisa menyediakan **layanan reaktif** - yaitu, respon terhadap insiden keamanan holistik dan **layanan preventif** - yaitu, upaya pendidikan keamanan holistik untuk mengurangi risiko insiden. Namun, dalam kebanyakan kasus, mereka akan membatasi daftar layanan mereka berdasarkan kapasitas dan memutuskan

untuk merujuk layanan tambahan ke tim lain.

Mengetahui Kapan Layanan Bisa Dilakukan oleh Organisasi dan Kapan Harus Dirujuk

Menentukan kapan suatu layanan dapat dilakukan oleh organisasi sendiri dan kapan harus dirujuk memerlukan evaluasi terhadap beberapa faktor kunci:

1. **Kapasitas dan Keahlian Internal**: Evaluasi kapasitas sumber daya manusia dan keahlian teknis yang ada di organisasi. Jika organisasi memiliki staf yang cukup dan berpengalaman dalam menangani jenis layanan tertentu, maka layanan tersebut bisa dilakukan secara internal. Namun, jika tidak ada keahlian yang memadai, lebih baik merujuk ke organisasi lain yang lebih kompeten.

2. **Sumber Daya dan Infrastruktur**: Pertimbangkan ketersediaan sumber daya dan infrastruktur yang diperlukan untuk menjalankan layanan. Misalnya, jika layanan memerlukan teknologi atau peralatan khusus yang tidak dimiliki organisasi, lebih baik merujuknya.

3. **Batasan Waktu dan Prioritas**: Tentukan batasan waktu yang tersedia untuk menangani layanan

tertentu. Jika organisasi sudah memiliki beban kerja yang tinggi dan tidak dapat menangani layanan tambahan secara efisien, lebih baik merujuk kasus tersebut untuk memastikan penanganan yang tepat waktu.

4. **SOP dan Prosedur Internal**: Periksa apakah ada SOP yang relevan untuk layanan tertentu. SOP yang jelas dan terperinci membantu memastikan layanan bisa diberikan dengan standar yang baik. Jika tidak ada SOP yang memadai, lebih baik merujuk layanan tersebut sampai SOP bisa disusun dan diterapkan.

5. **Risiko dan Dampak**: Pertimbangkan risiko dan dampak yang mungkin timbul jika layanan dilakukan secara internal. Jika risiko terlalu tinggi atau dampak negatifnya signifikan, lebih baik merujuk layanan tersebut. Ini juga mencakup risiko keamanan bagi staf dan penerima manfaat.

6. **Kolaborasi dan Jaringan**: Manfaatkan jaringan dan kolaborasi dengan organisasi lain. Jika ada organisasi mitra yang memiliki spesialisasi dalam layanan tertentu, lebih efisien untuk merujuk kasus tersebut untuk memastikan penerima manfaat mendapatkan dukungan terbaik.

7. **Umpan Balik dan Evaluasi**: Kumpulkan umpan balik dari penerima manfaat dan lakukan evaluasi berkala terhadap layanan yang diberikan. Hal ini membantu mengidentifikasi area di mana organisasi unggul dan area yang memerlukan dukungan dari luar.

Dengan mempertimbangkan faktor-faktor di atas, organisasi dapat membuat keputusan yang tepat kapan layanan bisa dilakukan secara internal dan kapan harus dirujuk untuk memastikan efektivitas dan kualitas dukungan yang diberikan kepada penerima manfaat.

Manajemen Informasi

Kebijakan Manajemen Informasi

Untuk memastikan bahwa informasi dikelola dengan aman dan efisien, organisasi perlu menerapkan kebijakan manajemen informasi yang komprehensif. Kebijakan ini mencakup klasifikasi informasi, penyimpanan dokumen, dan pembagian informasi berdasarkan kebutuhan dan sensitivitas data.

Ketika Menjadi Lembaga yang Menangani Kasus Secara Langsung

1. **Dokumen yang Perlu Disimpan**:
    - **Data Pribadi Penerima Manfaat**: Informasi pribadi yang penting untuk proses penanganan kasus.
    - **Detail Kasus**: Semua dokumen terkait dengan kasus, termasuk laporan insiden, bukti, dan catatan komunikasi.
    - **Riwayat Tindakan**: Catatan tindakan yang telah diambil, hasil intervensi, dan tindak lanjut yang dilakukan.

2. **Dokumen atau Informasi yang Perlu Dibagikan**:
    - **Informasi Publik**: Informasi yang tidak sensitif dan dapat didistribusikan kepada publik untuk kesadaran umum atau kampanye publik.
    - **Informasi Rahasia**: Hanya dibagikan kepada tim internal dan pihak ketiga terpercaya yang terlibat langsung dalam kasus, berdasarkan kebutuhan, setelah menandatangani perjanjian *non-disclosure.*

Ketika Menjadi Lembaga yang Merujuk Kasus

1. **Dokumen yang Perlu Disimpan**:
    - **Data Pribadi Penerima Manfaat**: Tetap menyimpan salinan informasi pribadi yang diperlukan untuk referensi masa depan.
    - **Detail Kasus**: Salinan laporan kasus awal dan riwayat komunikasi dengan penerima manfaat dan organisasi rujukan.
    - **Catatan Rujukan**: Dokumen yang

mencatat alasan rujukan, detail organisasi yang menerima rujukan, dan konfirmasi penerimaan kasus.

2. **Dokumen atau Informasi yang Perlu Dibagikan**:
    - **Informasi Kasus yang Relevan**: Hanya informasi yang relevan dan diperlukan oleh organisasi rujukan untuk menangani kasus dengan efektif.
    - **Data Pribadi dengan Izin**: Informasi pribadi penerima manfaat hanya dibagikan setelah mendapatkan izin dari yang bersangkutan dan setelah memastikan bahwa organisasi rujukan memiliki mekanisme perlindungan data yang memadai.

Dokumen yang Diperlukan untuk Memberikan Rujukan

- **Surat Pengantar Rujukan**: Surat resmi yang menjelaskan alasan rujukan dan memberikan ringkasan singkat tentang kasus.
- **Formulir Rujukan**: Formulir yang mencakup informasi dasar tentang penerima manfaat, detail kasus, dan kontak penting.

- **Persetujuan Penerima Manfaat**: Dokumen persetujuan dari penerima manfaat untuk merujuk kasus dan membagikan informasi pribadi mereka dengan organisasi rujukan.
- **Catatan Komunikasi**: Salinan komunikasi sebelumnya dengan penerima manfaat yang relevan dengan kasus.
- **Informasi Tambahan**: Dokumen tambahan yang mungkin diperlukan oleh organisasi rujukan untuk memberikan dukungan yang optimal, seperti laporan medis atau bukti pendukung lainnya (apabila diperlukan).

Dengan mengimplementasikan kebijakan manajemen informasi yang jelas, organisasi dapat memastikan bahwa data dikelola dengan aman dan efisien, baik dalam menangani kasus secara langsung maupun saat merujuknya ke organisasi lain.

Lembaga Rujukan

Internasional		
Nama Lembaga	**Jenis Layanan**	**Kontak**
1. Digital Defender Partnership 2. Access Now	Digital	https://www.digitaldefenders.org/ https://www.accessnow.org/help/
3. Front Line Defender 4. IREX	Holistik	https://www.frontlinedefenders.org/en/contact-us https://www.irex.org/project/safe-securing-access-free-expression
Nasional		
Nama Lembaga	**Jenis Layanan**	**Kontak**
1. SAFENet 2. AwasKBGO 3. TaskForce KBGO	Digital	https://safenet.or.id/id/kontak/ https://awaskbgo.id/layanan/ https://linktr.ee/taskforcekbgo
4. Yayasan Pulih 5. TigaGenerasi	Psikologi	https://www.yayasanpulih.org/our-services/layanan-konseling-psikologi https://www.tigagenerasi.id/kontak-kami

6. KOMPAKS 7. FPL 8. Perempuan Berkisah 9. Arus Pelangi 10. CRM	Psikoso-sial	kompaks@protonmail.com https://fpl.or.id/kontak/ https://linktr.ee/Perempuan-Berkisah https://aruspelangi.or.id/pen-gaduan-kasus/ https://crm-consortium.org/lembaga-pendamping/konsor-sium-crisis-response-mecha-nismcrm/
11. Yayasan Lembaga Bantuan Hukum Indonesia 12. LBH Masyarakat 13. LBH Pers	Hukum	https://ylbhi.or.id/ https://lbhmasyarakat.org/ https://lbhpers.org/

Referensi

1. TechCare_Guide_en.pdf (digitaldefenders.org)
2. irex.org/sites/default/files/node/resource/SAFE Basic Training Curriculum - Bahasa.pdf
3. the Digital First Aid Kit! | Digital First Aid Kit
4. https://advokasi.aji.or.id/safety.html
5. https://safenet.or.id/id/category/publikasi/panduan/
6. https://awaskbgo.id/publikasi/
7. https://www.frontlinedefenders.org/
8. https://www.accessnow.org/

Glosarium

No	Kata	Arti/ Makna dalam KBBI
1.	*Back up*	Membuat salinan cadangan.
2.	*Boundaries*	Batasan, garis tak terlihat yang memisahkan diri kita dari orang lain, lingkungan dan situasi.
3.	*Burnout*	Kelelahan fisik, emosional, dan mental.
4.	*Cloud*	Layanan yang menggunakan sekelompok komputer jaringan yang bekerja bersama sebagai super-komputer virtual untuk melakukan tugas besar atau intensif data.
5.	*Coping*	Upaya seseorang untuk mengatasi stres.
6.	*Debriefing*	Proses diskusi dan analisis yang dilakukan setelah suatu kegiatan selesai.
7.	*Detox digital*	Mengurangi atau membatasi penggunaan perangkat teknologi.

8.	*Digital*	Berhubungan dengan angka-angka untuk sistem perhitungan tertentu; berhubungan dengan penomoran.
9.	*Digital footprint*	Kumpulan data yang tertinggal setelah seseorang beraktivitas di internet.
10.	*Doxing*	Tindakan menyebarkan informasi pribadi seseorang tanpa izin.
11.	*Email*	Surat elektronik.
12.	Enkripsi data	Metode untuk mengubah data yang dapat dibaca menjadi format yang tidak dapat dibaca.
13.	*Exit*	Penyerang mengeksploitasi informasi atau akses yang telah diperoleh untuk mencapai tujuan mereka, seperti mencuri data, uang, atau menyebabkan kerusakan pada sistem.
14.	*Grounding*	Teknik terapi untuk menenangkan diri dan mengalihkan perhatian dari perasaan negatif.
15.	Holistik	Secara keseluruhan.

16.	*Hook*	Penyerang mulai berinteraksi dengan target untuk membangun kepercayaan. Ini bisa melalui *email,* telepon, atau pertemuan tatap muka.
17.	*Login*	Memulai akses ke sistem komputer dengan memasukan nama dan kata sandi atau perintah tertentu.
18.	*Log out*	Keluar; mengakhiri akses ke sistem komputer atau situs web.
19.	*Malware*	Program komputer yang dibuat dengan tujuan jahat.
20.	*Malware-bytes*	Sistem untuk pemindaian virus untuk memeriksa adanya ancaman pada memori sistem komputer dengan kecepatan tinggi.
21.	Misoginis	Orang yang membenci wanita (perempuan).
22.	*Non-disclosure*	Perjanjian hukum yang mengatur penggunaan informasi rahasia selama kerjasama berlangsung.
23.	*Patch*	Pembaruan perangkat lunak atau sistem operasi.

24.	Peretasan	Akses tanpa izin ke data dalam suatu slstem atau komputer.
25.	*Phishing*	Penipuan digital yang dilakukan untuk mendapatkan informasi pribadi seseorang secara tidak sah.
26.	*Play*	Penyerang mengembangkan hubungan dengan target untuk mendapatkan lebih banyak informasi atau akses. Mereka mungkin menggunakan cerita palsu atau skenario yang meyakinkan untuk menipu target.
27.	*Platform*	Rencana kerja; program; pernyataan sekelompok orang tentang prinsip.
28.	*Private*	Pribadi, tersendiri.
29.	Siber	Sistem komputer dan informasi atau dunia maya.
30.	Sistem *buddy*	Strategi keselamatan dan dukungan yang melibatkan dua orang atau lebih.

31.	*Tailgating* atau *baiting*	Menumpang atau tindakan yang tidak sah untuk mendapatkan akses ke sistem komputer dengan cara mengikuti atau mengamati orang lain yang memiliki akses sah.
32.	*Online*	Dalam jaringan, terhubung melalui jejaring komputer, internet dan sebagainya.
33.	*Web phising*	Penipuan dalam jaringan yang dilakukan melalui website.
34.	*Windows Defender*	Sitem untuk pemindaian virus untuk memeriksa adanya ancaman pada memori sistem komputer dengan kecepatan tinggi.

Norwegian Embassy
Jakarta

humanis
Igniting agency, inspiring change