BUKU PANDUAN KEAMANAN DIGITAL

Panduan Keamanan Digital
untuk Organisasi Masyarakat Sipil di Sumatera Utara

Kontributor
LBH Medan | WALHI Sumatera Utara | SahDar | Bakumsu | Yayasan Srikandi Lestari | Aliansi Sumut Bersatu | Petrasu | AJI Medan | AMAN Sumut | KontraS Sumatera Utara

Buku ini berisi panduan Keamanan Digital untuk Organisasi Masyarakat Sipil di Sumatera Utara. Panduan ini bertujuan untuk meningkatkan kesadaran dan ketahanan digital terhadap berbagai ancaman siber dengan pendekatan praktis dan sesuai dengan kebutuhan organisasi.

This book contains Digital Security guidelines for Civil Society Organizations in North Sumatra. This guide aims to increase awareness and digital resilience against various cyber threats with a practical approach and according to the needs of the organization.

BAB 1
PENDAHULUAN

CHAPTER 1
INTRODUCTION

Latar Belakang

Sebagai upaya meminimalisir ancaman dan serangan digital di era perkembangan teknologi informasi, maka setiap organisasi seharusnya memiliki panduan manajemen sistem keamanan digital. Hal tersebut sangat penting dilakukan guna untuk mencegah, menangani, dan memulihkan ancaman digital. Panduan ini sangat membantu dalam menjalankan aktivitas sehari-hari, begitu pula bagi kerja-kerja organisasi masyarakat sipil (OMS).

Sebagian besar OMS yang berada di Sumatera Utara melakukan kerja-kerja untuk pemajuan hak asasi manusia dan demokrasi. Aktivitas yang dilakukan erat dengan isu-isu sensitif berkaitan dengan pelanggaran hak asasi manusia. Adapun aktivitas digital yang dilakukan berupa kampanye publik, riset, advokasi, penanaman nilai-nilai organisasi, dan lainnya. Tentu hal ini menjadi perhatian bagi organisasi untuk memiliki panduan keamanan digital.

Background

In an effort to minimize digital threats and attacks in the era of information technology development, every organization should have a digital security system management guide. It is very important to prevent, handle and recover from digital threats. This guide is very helpful in carrying out daily activities, as well as for the work of civil society organizations (CSOs).

Most of the CSOs in North Sumatra work for the promotion of human rights and democracy. The activities carried out are closely related to sensitive issues related to human rights violations. The digital activities carried out are in the form of public campaigns, research, advocacy, instilling organizational values, and others. Of course this is a concern for organizations to have digital security guidelines.

Tujuan

1. Meningkatkan kesadaran untuk keamanan di ruang digital.
2. Melindungi data pribadi atau organisasi dalam menjalankan aktivitasnya.
3. Mencegah serangan siber seperti malware, ransomware, dan phising yang dapat merusak sistem dan terjadinya pencurian data.
4. Mendeteksi adanya risiko keamanan siber dalam kerja-kerja OMS.
5. Menangani insiden serangan siber dan upaya pencurian data.
6. Menjadi pedoman keamanan digital dalam kerja-kerja OMS.

Objectives

1. Raise awareness for security in the digital space.
2. Protect personal or organizational data in carrying out its activities.
3. Preventing cyber-attacks such as malware, ransomware, and phishing that can damage the system and cause data theft.
4. Detecting cybersecurity risks in the work of CSOs.
5. Handle incidents of cyber-attacks and data theft attempts.
6. Serve as a digital security guideline for CSO work.

Ruang Lingkup

Panduan keamanan digital ini sangat dibutuhkan bagi OMS untuk melakukan pengamanan digital yang berbentuk data, informasi, perangkat lunak dan perangkat keras. Panduan ini terikat kepada staf, relawan dan dampingan di setiap organisasi.

Scope

This digital security guide is essential for CSOs to secure digital data, information, software and hardware. This guide is bound to the staff, volunteers and assistants in each organization.

BAB 2
KEBIJAKAN UMUM KEAMANAN DIGITAL

CHAPTER 2
DIGITAL SECURITY COMMON POLICY

Melihat besarnya ancaman serangan digital yang dihadapi OMS, maka diperlukan adanya komitmen dan kerja sama dari staf, relawan, dan dampingan untuk mengamankan aset digital organisasi. Oleh karena itu, diperlukan adanya kesadaran, kehati-hatian, dan ketelitian dalam menjaga keamanan digital organisasi. Hal tersebut wajib dijalankan dan dipatuhi dengan etika, integritas, serta tunduk terhadap aturan yang berlaku di dalam organisasi.

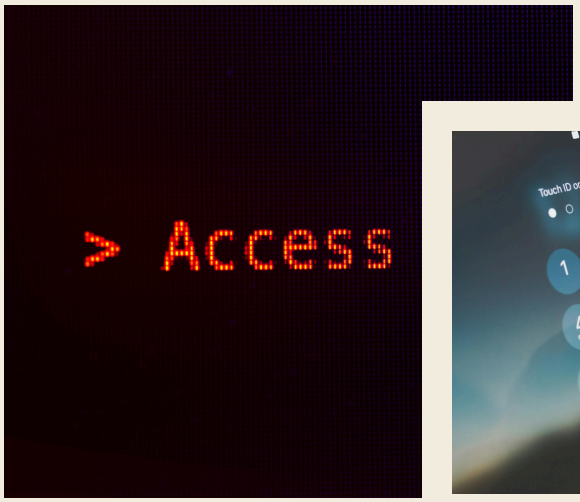
Considering the threat of digital attacks faced by CSOs, there is a need for commitment and cooperation from staff, volunteers, and assistants to secure the organization's digital assets. Therefore, there is a need for awareness, caution, and thoroughness in maintaining the organization's digital security. This must be carried out and adhered to with ethics, integrity, and compliance with the rules that apply in the organization.

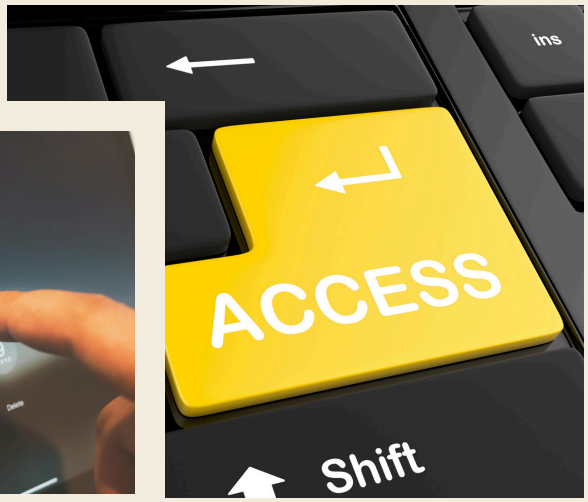
BAB 3

KOMPONEN UTAMA PANDUAN

CHAPTER 3

KEY COMPONENTS OF THE GUIDE





Manajemen Aset digital dan Akses

1. Setiap aset digital (email, akun media sosial, website, dan produk digital seperti dokumen, gambar, audio, video, uang elektronik dan lainnya) organisasi seperti wajib didaftarkan dan didokumentasikan secara kelembagaan.
2. Setiap staf, relawan dan dampingan wajib melakukan verifikasi dua langkah pada akun media sosial, email dan aplikasi perpesanan.
3. Staf pengelola akun organisasi wajib mengakhiri sesi (log out) setelah selesai digunakan.
4. Akses atas aset digital diberikan dan dikembalikan sesuai dengan peran dan tanggung jawab di dalam organisasi.
5. Setiap pergantian dan pengalihan tanggung jawab atas akses digital wajib dilakukan perubahan kata sandi.

Digital Asset Management and Access

1. Every digital asset (email, social media accounts, websites, and digital products such as documents, images, audio, video, electronic money, etc.) of such organizations must be registered and documented institutionally.
2. All staff, volunteers and mentees are required to have two-step verification on social media accounts, emails and messaging applications.
3. The organization's account management staff must end the session (log out) after completion of use.
4. Access to digital assets is granted and returned in accordance with roles and responsibilities within the organization.
5. very change and transfer of responsibility for digital access requires a password change.

Kebijakan Kata Sandi

1. Sandi minimal 12 karakter, mengandung kombinasi huruf besar, kecil, angka, dan simbol, dapat menggunakan metode enkripsi atau metode jembatan keledai.
2. Ganti kata sandi secara berkala minimal setiap 3 bulan.
3. Gunakan aplikasi password manager untuk mengelola kata sandi.
4. Setiap aset digital wajib menggunakan kata sandi yang berbeda.
5. Penanggung jawab aset digital wajib merahasiakan informasi terkait aset digital.
6. Setiap kata sandi untuk aset digital wajib diperkuat dengan autentikasi dua langkah, baik menggunakan perangkat lunak maupun perangkat keras. – digunakan untuk pasal lain di bawah

Password Policy

1. Passwords must be at least 12 characters long, contain a combination of uppercase and lowercase letters, numbers and symbols, and can use the encryption method or the donkey bridge method.
2. Change passwords regularly at least every 3 months.
3. Use a password manager application to manage passwords.
4. Each digital asset must use a different password.
5. The person in charge of digital assets must keep information related to digital assets confidential.
6. Each password for digital assets must be reinforced with two-step authentication, either using software or hardware. - used for other articles below.

Pengelolaan Perangkat dan Aplikasi

1. Mengunduh antivirus yang terpercaya pada semua perangkat digital (laptop, tablet, perangkat seluler dan perangkat keras lainnya)
2. Lakukan pembaruan dan peningkatan sistem operasi, aplikasi, perangkat lunak dan perangkat keras secara rutin atau berkala.
3. Gunakan perangkat lunak dan perangkat keras yang resmi.
4. Tidak meminjamkan perangkat digital kepada pihak lain.

Device and Application Management

1. Download a trusted antivirus on all digital devices (laptops, tablets, mobile devices and other hardware)
2. Perform regular or periodic updates and upgrades of operating systems, applications, software and hardware.
3. Use authorized software and hardware.
4. Do not lend digital devices to other parties.

Keamanan seluler

1. Aktifkan kunci layar dan enkripsi perangkat

    - Gunakan kata sandi untuk masuk ke perangkat seluler (handphone dan tablet).
    - Penguncian layar untuk perangkat seluler wajib menggunakan kata sandi. Tidak boleh menggunakan biometrik dan pola (pattern) untuk penguncian layer.
    - Setiap kata sandi untuk aset digital wajib diperkuat dengan autentikasi dua langkah, baik menggunakan perangkat lunak maupun perangkat keras. – digunakan untuk pasal lain di bawah.

Mobile Security

1. Enable screen lock and device encryption

    - Use a password to log in to mobile devices (mobile phones and tablets).
    - Screen lock for mobile devices must use a password. Biometrics and patterns should not be used for layer locking.
    - Any passwords for digital assets must be reinforced with two-step authentication, whether using software or hardware. - used for other articles below.

2.Unduh aplikasi dari penyedia resmi (Google Play Store, App Store, App Gallery dan Microsoft Store).

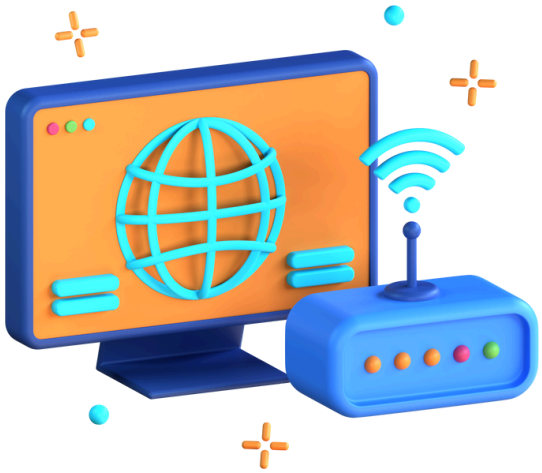
3. Koneksi Nirkabel

- Nonaktifkan koneksi nirkabel (Wi-Fi, Bluetooth), jika tidak sedang digunakan.
- Hapus Riwayat koneksi Wi-Fi yang pernah digunakan.
- Batasi penggunaan Wi-Fi publik ketika melakukan kerja-kerja organisasi.
- Tidak menggunakan Wi-Fi publik ketika melakukan transaksi keuangan daring.
- Menggunakan aplikasi VPN saat mengakses asset digital organisasi (optional).
- Virtual private network (VPN) adalah jaringan virtual personal yang berguna untuk menembus blokir atau menyembunyikan lokasi kita ketika mengakses Internet.
- Gunakan VPN jika mengakses Internet di tempat umum seperti kafe, hotel, bandara, dan lain-lain.
- Pilih VPN yang sudah dikenal dan dipercaya oleh komunitas, seperti ProtonVPN, NordVPN, dan semacamnya.

2. Download apps from authorized providers (Google Play Store, App Store, App Gallery and Microsoft Store).

3. Wireless Connection

- Disable wireless connections (Wi-Fi, Bluetooth), if not in use.
- Clear the history of used Wi-Fi connections.
- Limit the use of public Wi-Fi when doing organizational work.
- Do not use public Wi-Fi when conducting online financial transactions.
- Use a VPN app when accessing the organization's digital assets (optional).
- A virtual private network (VPN) is a personal virtual network that is useful for bypassing blocks or hiding your location when accessing the Internet.
- Use a VPN when accessing the Internet in public places such as cafes, hotels, airports, and others.
- Choose a VPN that is known and trusted by the community, such as ProtonVPN, NordVPN, and the like.



4. Menggunakan aplikasi VPN saat mengakses asset digital organisasi (optional).

- Virtual private network (VPN) adalah jaringan virtual personal yang berguna untuk menembus blokir atau menyembunyikan lokasi kita ketika mengakses Internet.
- Gunakan VPN jika mengakses Internet di tempat umum seperti kafe, hotel, bandara, dan lain-lain.
- Pilih VPN yang sudah dikenal dan dipercaya oleh komunitas, seperti ProtonVPN, NordVPN, dan semacamnya.

4. Use a VPN application when accessing the organization's digital assets (optional).

- A virtual private network (VPN) is a personal virtual network that is useful for bypassing blocks or hiding your location when accessing the Internet.
- Use a VPN when accessing the Internet in public places such as cafes, hotels, airports, and others.
- Choose a VPN that is known and trusted by the community, such as ProtonVPN, NordVPN, and the like.

Keamanan Email

1. Waspadai email phishing dengan tautan mencurigakan.
   - Mengganti password email secara berkala setiap 3 (tiga) bulan dan gunakan kata sandi yang berbeda pada setiap email dan akun sosial media.
   - Tidak membuka lampiran dari pengirim yang tidak dikenal.
   - Melakukan pemindaian sebelum membuka lampiran yang diterima

Email Security

1. Beware of phishing emails with suspicious links.
   - Change email passwords regularly every 3 (three) months and use different passwords for each email and social media account.
   - Do not open attachments from unknown senders.
   - Perform scanning before opening attachments received

2. Gunakan email terenkripsi untuk komunikasi yang mengandung data penting dan rahasia.

- Gunakan layanan email yang menyediakan fungsi enkripsi seperti Protonmail.
- Gunakan kata sandi untuk lampiran dokumen yang bersifat penting dan rahasia (menggunakan zip yang diproteksi dengan kata sandi)

3. Setiap kata sandi untuk aset digital wajib diperkuat dengan autentikasi dua langkah, baik menggunakan perangkat lunak maupun perangkat keras. – digunakan untuk pasal lain di bawah.

Keamanan Media Penyimpanan Eksternal

1. Batasi penggunaan media penyimpanan eksternal dalam organisasi
2. Lakukan pemindaian antivirus pada setiap perangkat penyimpanan eksternal (flashdisk, eksternal hardisk, dan kartu memori) sebelum digunakan.
3. Lakukan prosedur enkripsi data dalam media penyimpanan eksternal.
4. Lakukan prosedur pelepasan (eject) sebelum mencabut media penyimpanan eksternal dari perangkat digital.

2. Use encrypted email for communications containing important and confidential data.

- Use an email service that provides encryption functions such as Protonmail.
- Use passwords for important and confidential document attachments (using password-protected zips).

3. Any passwords for digital assets must be reinforced with two-step authentication, whether using software or hardware. - used for other articles below.

External Storage Media Security

1. Limit the use of external storage media within the organization
2. Perform an antivirus scan on each external storage device (flash drives, external hard drives, and memory cards) before use.
3. Perform data encryption procedures on external storage media.
4. Perform the eject procedure before unplugging the external storage media from the digital device.

Keamanan Media Sosial

1. Batasi penyebaran informasi pribadi di media sosial (identitas diri, kontak pribadi, informasi keuangan, data Lokasi, aktivitas digital, informasi Kesehatan, data masyarakat yang didampingi, dan sensitif lainnya).
2. Tinjau dan kelola pengaturan privasi secara berkala. Meninjau izin pada aplikasi sosial media jika tidak diperlukan, (akses kamera, mikrofon, pengenalan wajah, lokasi dan fitur lainnya)
3. Bijak dalam mengunggah konten dalam akun sosial media Memastikan data pribadi atau organisasi tidak terbuka untuk publik, (Pindah ke insiden)
4. Waspadai rekayasa sosial (social engineering).
5. Tidak membuka tautan atau file dari sumber yang tidak dikenal;
6. Tidak membagikan password atau OTP (one time password).

Social Media Security

1. Limit the sharing of personal information on social media (personal identity, personal contacts, financial information, location data, digital activity, health information, data on assisted communities, and other sensitive information).
2. Review and manage privacy settings regularly. Review permissions on social media applications if not needed, (access to camera, microphone, facial recognition, location and other features)
3. Be wise in uploading content on social media accounts Ensure personal or organizational data is not public, (Move to incident)
4. Beware of social engineering.
5. Do not open links or files from unknown sources;
6. Do not share passwords or OTP (one time password).

Panggilan Video Online

1. Gunakan platform video call yang aman dan terenkripsi.
2. Gunakan aplikasi panggilan video sesuai dengan kebutuhan dan kondisi.
3. Tidak membagikan tautan rapat daring di ruang publik.
4. Gunakan kata sandi untuk mengakses pertemuan online.
5. Aktifkan fitur ruang tunggu (waiting room) untuk menyaring peserta.
6. Jika rapat yang diadakan adalah rapat organisasi atau lembaga, peserta wajib mengaktifkan kamera dan menuliskan nama serta asal lembaga.

Online Video Calls

1. Use a secure and encrypted video calling platform.
2. Use video calling apps according to your needs and circumstances.
3. Do not share online meeting links in public spaces.
4. Use passwords to access online meetings.
5. Enable the waiting room feature to screen participants.
6. If the meeting is an organizational or institutional meeting, participants must activate the camera and write their name and institutional origin.

Pertahanan terhadap Malware

1. Selalu aktifkan dan perbaharui antivirus.

- Gunakan antivirus pada perangkat (handphone dan laptop) untuk mengetahui atau mencegah adanya virus di dalam perangkat.
- Pindai perangkat secara berkala untuk mengantisipasi jika ada aplikasi atau perangkat lunak berbahaya di dalam perangkat.

1. Unduh aplikasi dari penyedia resmi (Google Play Store, App Store, App Gallery dan Microsoft Store).
2. Lakukan pemindaian berkala pada asset digital pribadi dan organisasi.

Pertahanan terhadap Malware

1. Always activate and update your antivirus.

- Use an antivirus on your devices (mobile phones and laptops) to detect or prevent viruses on your devices.
- Scan the device regularly to anticipate if there are malicious applications or software on the device.

1. Download apps from authorized providers (Google Play Store, App Store, App Gallery and Microsoft Store).
2. Conduct regular scans of personal and organizational digital assets.

Pengendalian Sambungan Internet

1. Gunakan jaringan internet terpercaya.

- Ketika di kantor, menggunakan wifi kantor
- Nonaktifkan koneksi nirkabel (Wi-Fi, Bluetooth), jika tidak sedang digunakan.
- Hapus Riwayat koneksi Wi-Fi yang pernah digunakan.
- Batasi penggunaan Wi-Fi publik ketika melakukan kerja-kerja organisasi.
- Tidak menggunakan Wi-Fi publik ketika melakukan transaksi keuangan daring.
- Menerapkan pengaturan koneksi internet sekali pakai untuk semua pengguna di lingkungan kantor (opsional).

2. Lindungi Wi-Fi dengan kata sandi yang kuat dan ubah kata sandi secara berkala.

- Mengganti kata sandi secara berkala 1 bulan sekali.
- Kata sandi wifi menggunakan kombinasi huruf besar, kecil, angka dan simbol.
- Menunjuk satu orang staf yang bertanggung jawab untuk mengganti kata sandi secara berkala.
- Menggunakan aplikasi password manager seperti Bitwarden dan keepass.
- Gunakan VPN saat mengakses sistem dari luar kantor.

Internet Connection Control

1. Use a trusted internet network.

- When in the office, use the office wifi
- Disable wireless connections (Wi-Fi, Bluetooth), if not in use.
- Delete the history of Wi-Fi connections that have been used.
- Limit the use of public Wi-Fi when doing organizational work.
- Do not use public Wi-Fi when conducting online financial transactions.
- Implement a single-use internet connection setting for all users in the office environment (optional).

2. Protect Wi-Fi with a strong password and change the password regularly.

- Change the password regularly once a month.
- The wifi password uses a combination of uppercase, lowercase letters, numbers and symbols.
- Appoint one staff member who is responsible for changing passwords regularly.
- Use password manager applications such as Bitwarden and keepass.
- Use VPN when accessing the system from outside the office.

Panduan Keamanan dan Pelaporan Masalah

1. Tunjuk petugas keamanan digital di organisasi, dengan kriteria:

- Telah mengikuti pelatihan keamanan digital.
- Minimal sudah bekerja di organisasi/lembaga selama 1 tahun.
- Memahami klasifikasi data (rahasia, umum, sangat penting).
- Mendapatkan rekomendasi dari 3 staf organisasi lainnya
- Bertanggung jawab.

2. Sediakan formulir pelaporan insiden keamanan yang berisi:
- Identifikasi jenis insiden keamanan siber
- Identifikasi penyebab terjadinya insiden siber/keamanan

3. Laporkan insiden keamanan siber kepada pimpinan untuk di tindak lanjuti.

4. Dokumentasikan dan evaluasi setiap insiden untuk pencegahan ke depan.

Security and Problem Reporting Guidelines

1. Appoint a digital security officer in the organization, with criteria:

- Has attended digital security training.
- Have worked at the organization/institution for at least 1 year.
- Understand the classification of data (confidential, general, very important).
- Get recommendations from 3 other organization staff
- Responsible.

2. Provide a security incident reporting form that contains:
- Identify the type of cyber security incident
- Identify the cause of the cyber/security incident.

3. Report cybersecurity incidents to leadership for follow-up.

4. Document and evaluate each incident for future prevention.

Kepatuhan

1. Tinjau regulasi perlindungan data yang berlaku (UU ITE dan PDP).
2. Update berdasarkan perubahan, dan menyesuaikan dengan panduan keamanan digital organisasi.
3. Sosialisasikan kebijakan keamanan digital kepada seluruh staf.
4. Lakukan pelatihan keamanan digital secara berkala; jika ada staf yang baru masuk dan jika ada perkembangan isu keamanan digital.

Compliance

1. Review applicable data protection regulations (ITE Law and PDP).
2. Update based on changes, and align with the organization's digital security guidelines.
3. Socialize the digital security policy to all staff.
4. Conduct regular digital security training; if new staff join and if there are developments in digital security issues.

Peran dan Tanggung Jawab

Peran	Tanggung Jawab
Koordinator Organisasi	Menjamin penerapan panduan
Penanggung jawab keamanan digital	Menjamin penerapan panduan
Semua Anggota	Mematuhi panduan dan melapor insiden

Roles and Responsibilities

Roles	Responsibilities
Organization Coordination	Ensure implementation of guidelines
In charge of digital security	Ensure implementation of guidelines
All the members	Follow guidelines and report incidents

BAB 4
PENUTUP

CHAPTER 4
CLOSING

Keamanan digital adalah kebutuhan mendasar di era informasi saat ini. Melalui panduan ini, kami berharap setiap pembaca dapat memahami langkah-langkah praktis untuk melindungi diri, data pribadi, dan komunitas dari risiko kejahatan siber yang terus berkembang. Namun, menjaga keamanan digital bukan hanya tanggung jawab individu, tetapi juga upaya kolektif yang membutuhkan dukungan banyak pihak, terutama Organisasi Masyarakat Sipil (OMS).

Sebagai bagian dari masyarakat sipil, OMS memiliki peran penting dalam mengedukasi, mendampingi, dan memperkuat kesadaran warga agar lebih waspada di ruang digital. Dengan diskusi komunitas, pelatihan bersama, hingga advokasi kebijakan perlindungan data, OMS dapat membantu menciptakan ekosistem digital yang aman, adil, dan memberdayakan semua orang.

Panduan ini diharapkan dapat menjadi bahan belajar bersama dalam berbagai kegiatan OMS. Mari saling mengingatkan, berbagi informasi, dan membangun solidaritas digital untuk menghadapi tantangan siber ke depan.

Terima kasih telah membaca. Bersama OMS dan masyarakat, mari wujudkan ruang digital yang aman, nyaman, dan bermanfaat bagi semua.

Digital security is a fundamental need in today's information era. Through this guide, we hope every reader can understand practical steps to protect themselves, their personal data, and their communities from the ever-evolving risks of cybercrime. However, maintaining digital security is not solely an individual responsibility; it is a collective effort that requires support from many parties, especially Civil Society Organizations (CSOs).

As an integral part of civil society, CSOs play a crucial role in educating, assisting, and strengthening public awareness to be more vigilant in the digital space. Through community discussions, joint training, and policy advocacy on data protection, CSOs help create a safe, fair, and empowering digital ecosystem for everyone.

This guide is intended to serve as a shared learning tool in various CSO activities. Let us remind one another, share information, and build digital solidarity to face future cyber challenges together.

Thank you for reading. Together with CSOs and the community, let's create a digital space that is safe, comfortable, and beneficial for all.

KONTRIBUTOR

Buku panduan Keamanan Digital ini lahir dari hasil kolaborasi dan semangat belajar para peserta Workshop Keamanan Digital yang diselenggarakan sebagai bagian dari upaya memperkuat literasi dan kesadaran akan pentingnya perlindungan data pribadi di era digital.

Para kontributor berasal dari berbagai latar belakang: aktivis masyarakat sipil, pegiat komunitas, pendamping warga, relawan organisasi sosial, hingga individu yang peduli dengan isu perlindungan privasi dan hak digital. Dalam proses workshop, para peserta tidak hanya menerima materi dan praktik langsung, tetapi juga terlibat aktif dalam merumuskan konten buku ini melalui diskusi, tukar pengalaman, dan berbagi praktik baik di komunitas masing-masing.

Sebagian besar dari mereka telah menerapkan pengetahuan yang didapat untuk memperkuat kapasitas komunitasnya dalam menghadapi tantangan dunia maya, baik melalui pelatihan, kampanye, maupun pendampingan warga.

Dengan semangat kolaborasi, para peserta berharap panduan ini dapat menjadi referensi praktis, mudah dipahami, dan bermanfaat luas, tidak hanya untuk individu, tetapi juga untuk organisasi masyarakat sipil, komunitas lokal, dan publik pada umumnya.

Kami mengucapkan terima kasih atas kontribusi ide, waktu, dan tenaga seluruh peserta workshop. Semoga karya bersama ini menjadi langkah kecil namun berarti dalam mewujudkan ruang digital yang lebih aman, adil, dan memberdayakan.

Contributor

LBH Medan | WALHI Sumatera Utara | SahDar | Bakumsu | Yayasan Srikandi Lestari | Aliansi Sumut Bersatu | Petrasu | AJI Medan | AMAN Sumut | KontraS Sumatera Utara