



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN
RISET, DAN TEKNOLOGI

LEMBAGA LAYANAN PENDIDIKAN TINGGI
WILAYAH I

Jalan Sempurna Tanjung Sari Medan 20132
Telepon : 061 – 8214878, 8210359, Fax : 8210360
Laman : <http://lldikti1.kemdikbud.go.id>

Nomor : 5827/LL1/KL.03/2024

25 September 2024

Lampiran : -

Perihal : Profil Risiko Keamanan Siber Sektor Pendidikan

Yth. Pimpinan Perguruan Tinggi Negeri dan Swasta
Di Lingkungan Lembaga Layanan Pendidikan Tinggi Wilayah I

Sebagai tindak lanjut surat Kepala Pusat Data dan Teknologi Informasi Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi nomor 3496/J1/TI.02.01/2024 tanggal 23 September 2024 tentang Profil Risiko Keamanan Siber Sektor Pendidikan bersama ini kami mengundang seluruh Perguruan Tinggi Swasta di Lingkungan Lembaga Layanan Pendidikan Tinggi Wilayah I untuk hadir dalam rangkaian kegiatan sebagai berikut.

- Workshop Profil Risiko Keamanan Siber Sektor Pendidikan**, dilaksanakan pada
hari, tanggal : Kamis, 26 September 2024
pukul : 09.00 – 12.00 WIB
tautan : <https://s.id/WorkshopRisk2024>
peserta : Perwakilan Pengelola TIK masing-masing Perguruan Tinggi di Indonesia
- Pengisian Survei Profil Risiko Keamanan Siber Sektor Pendidikan**, dilaksanakan pada
hari, tanggal : Kamis – Selasa, 26 September – 15 Oktober 2024
tautan : <https://s.id/ProfilRisk2024>
- Diseminasi Laporan Hasil Survei Profil Risiko Keamanan Siber Sektor Pendidikan**, dilaksanakan pada
hari, tanggal : Kamis, 24 Oktober 2024
pukul : 09.00 – 12.00 WIB
tautan : <https://s.id/HasilRisk2024>
peserta : Perwakilan Pengelola TIK masing-masing Perguruan Tinggi.

Kami mohon Saudara berkenan menugaskan Pengelola TIK di Perguruan Tinggi Saudara. Untuk informasi dan koordinasi lebih lanjut, saudara dapat menghubungi Endro Joko Wibowo (0812-1618-3206) sebagai narahubung. Atas perhatian dan kerja samanya, kami ucapkan terima kasih

Atas perhatian dan kerja sama Saudara, kami ucapkan terima kasih.

Kepala,



Saiful Anwar Matondang
NIP 196807261993031003



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI

PUSAT DATA DAN TEKNOLOGI INFORMASI

Jalan R.E. Martadinata, Tromol Pos 7/CPA, Ciputat, Tangerang Selatan 15411
Telepon (021) 7418808; Laman pusdatin.kemdikbud.go.id; Posel pusdatin@kemdikbud.go.id

Nomor : 3496/J1/TI.02.01/2024
Lampiran : Satu dokumen
Hal : Profil Risiko Keamanan Siber Sektor Pendidikan

23 September 2024

Yth. Pimpinan Satuan Kerja
Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi
(daftar terlampir)

Sebagai tindak lanjut surat Direktur Keamanan Siber dan Sandi Pembangunan Manusia, Badan Siber dan Sandi Negara nomor 5416/BSSN/D3/PS.02.02/09/2024 tanggal 17 September 2024 tentang Penyusunan Profil Risiko Keamanan Siber Sektor Pendidikan Tahun 2024 dan sebagai kelanjutan dari *Open Meeting* Kegiatan Penyusunan Profil Risiko Keamanan Siber di Sektor Pendidikan yang dilaksanakan pada 19 September 2024 lalu, bersama ini kami bermaksud mengundang seluruh Perguruan Tinggi di Indonesia untuk hadir dalam rangkaian kegiatan sebagai berikut.

- 1. Workshop Profil Risiko Keamanan Siber Sektor Pendidikan**, dilaksanakan pada
hari, tanggal : Kamis, 26 September 2024
pukul : 09.00 – 12.00 WIB
tautan : <https://s.id/WorkshopRisk2024>
peserta : Perwakilan Pengelola TIK masing-masing Perguruan Tinggi di Indonesia
- 2. Pengisian Survei Profil Risiko Keamanan Siber Sektor Pendidikan**, dilaksanakan pada
hari, tanggal : Kamis – Selasa, 26 September – 15 Oktober 2024
tautan : <https://s.id/ProfilRisk2024>
- 3. Diseminasi Laporan Hasil Survei Profil Risiko Keamanan Siber Sektor Pendidikan**, dilaksanakan pada
hari, tanggal : Kamis, 24 Oktober 2024
pukul : 09.00 – 12.00 WIB
tautan : <https://s.id/HasilRisk2024>
peserta : Perwakilan Pengelola TIK masing-masing Perguruan Tinggi.

Catatan :

- UU ITE No. 11 Tahun 2008 Pasal 5 Ayat 1 "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti yang sah."
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh BSR

Kami mohon Saudara berkenan meneruskan undangan ini ke Perguruan-Perguruan Tinggi di unit kerja Saudara. Untuk informasi dan koordinasi lebih lanjut, kami menugasi Endro Joko Wibowo (0812-1618-3206) sebagai narahubung.

Atas perhatian dan kerja samanya, kami ucapkan terima kasih.

Kepala Pusat Data dan Teknologi
Informasi,



Yudhistira Nugraha
NIP 198106292006041005

Tembusan:

1. Sekretaris Jenderal
2. Direktur Jenderal Pendidikan Tinggi, Riset, dan Teknologi
3. Direktur Jenderal Pendidikan Vokasi

Lampiran Surat

Nomor : 3496/J1/TI.02.01/2024
Tanggal : 23 September 2024
Hal : *Workshop* Profil Risiko Keamanan Siber Sektor Pendidikan

Yth.

1. Sekretaris Direktorat Jenderal Pendidikan Tinggi, Riset, dan Teknologi
2. Sekretaris Direktorat Jenderal Pendidikan Vokasi
3. Kepala LLDIKTI Wilayah I, Medan
4. Kepala LLDIKTI Wilayah II, Palembang
5. Kepala LLDIKTI Wilayah III, Jakarta
6. Kepala LLDIKTI Wilayah IV, Bandung
7. Kepala LLDIKTI Wilayah V, Yogyakarta
8. Kepala LLDIKTI Wilayah VI, Semarang
9. Kepala LLDIKTI Wilayah VII, Surabaya
10. Kepala LLDIKTI Wilayah VIII, Denpasar
11. Kepala LLDIKTI Wilayah IX, Makassar
12. Kepala LLDIKTI Wilayah X, Padang
13. Kepala LLDIKTI Wilayah XI, Banjarmasin
14. Kepala LLDIKTI Wilayah XII, Ambon
15. Kepala LLDIKTI Wilayah XIII, Aceh
16. Kepala LLDIKTI Wilayah XIV, Biak Numfor
17. Kepala LLDIKTI Wilayah XV, Kupang
18. Kepala LLDIKTI Wilayah XVI, Gorontalo
19. Kepala LLDIKTI Wilayah XVII, Pekanbaru



BADAN SIBER DAN SANDI NEGARA

Jalan Raya Muchtar Nomor 70, Kel. Bojongsari Lama, Kec. Bojongsari, Depok 16518

Telepon (021) 77973360, Faksimile (021) 78844104, 77973579

Website: <https://www.bssn.go.id>, E-mail: humas@bssn.go.id

Nomor : 5416/BSSN/D3/PS.02.02/09/2024 Depok, 17 September 2024
Sifat : Biasa
Lampiran : 1 (satu) berkas
Hal : Penyusunan Profil Risiko Keamanan Siber
Sektor Pendidikan Tahun 2024

Yth. Kepala Pusat Data dan Informasi (Pusdatin)
Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi (Kemdikbudristek) RI

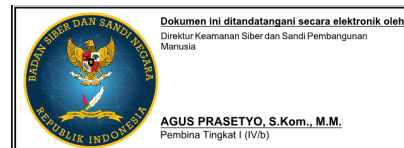
di –
Jakarta

1. Dasar:
 - a. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
 - b. Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik;
 - c. Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik.
2. Merujuk dasar tersebut di atas, Badan Siber dan Sandi Negara bermaksud berkolaborasi dengan Kemdikbudristek untuk melaksanakan kegiatan penyusunan profil risiko keamanan siber di sektor Pendidikan. Kegiatan ini merupakan tindak lanjut dari rangkaian kegiatan yang dilakukan di tahun 2022 dan 2023 khususnya profil risiko keamanan siber pada Perguruan Tinggi. Kegiatan ini bertujuan untuk mengetahui tren risiko keamanan siber serta kesiapan tata kelola keamanan siber yang diterapkan oleh pemangku kepentingan di sektor Pendidikan.
3. Rangkaian kegiatan penyusunan profil risiko keamanan siber di sektor Pendidikan terdiri dari:
 - a. *Workshop* Profil Risiko Keamanan Siber Sektor Pendidikan, dilaksanakan pada:

Hari / Tanggal	: Kamis, 26 September 2024
Waktu	: 09.00 – 12.00 WIB
Tempat	: Daring (<i>online</i>) dengan tautan akses https://s.id/WorkshopRisk2024
Peserta	: Perwakilan Pengelola TIK masing-masing Perguruan Tinggi di Indonesia

- b. Pengisian Survei Profil Risiko Keamanan Siber Sektor Pendidikan, dilaksanakan pada:
- Tanggal : 26 September – 15 Oktober 2024
- Metode : Daring (*online*) dengan tautan akses
<https://s.id/ProfilRisk2024>
- c. Diseminasi Laporan Hasil Survei Profil Risiko Keamanan Siber Sektor Pendidikan, direncanakan pada:
- Hari / Tanggal : Kamis, 24 Oktober 2024
- Waktu : 09.00 – 12.00 WIB
- Tempat : Daring (*online*) dengan tautan akses
<https://s.id/HasilRisk2024>
- Peserta : Perwakilan Pengelola TIK masing-masing Perguruan
4. Sehubungan dengan rangkaian kegiatan di atas, kami memohon bantuan agar Kemendikbudristek dapat mengundang seluruh Perguruan Tinggi di Indonesia untuk dapat mengikuti rangkaian Penyusunan Profil Risiko Keamanan Siber Sektor Pendidikan.
5. Demikian, atas perhatian dan kerjasamanya disampaikan terima kasih.

a.n. Kepala Badan Siber dan Sandi Negara
Deputi Bidang Keamanan Siber dan Sandi
Pemerintahan dan Pembangunan Manusia,
u.b.



Tembusan:

1. Kepala Badan Siber dan Sandi Negara;
2. Wakil Kepala Badan Siber dan Sandi Negara;
3. Sekretaris Utama Badan Siber dan Sandi Negara;
4. Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia;
5. Inspektur Badan Siber dan Sandi Negara.

Survei Identifikasi Aset dan Risiko Keamanan Informasi & Siber Sektor Pendidikan Tahun 2024

Disclaimer

- Survei Profil Risiko Keamanan Informasi dan Siber sektor Pendidikan bertujuan untuk mendata dan mengetahui profil risiko keamanan dan siber pada setiap penyelenggara sistem elektronik yang menjadi *stakeholder* Direktorat Keamanan Siber dan Sandi Pembangunan Manusia.
- Data dari hasil pengisian survei ini sepenuhnya digunakan sebagai data dukung untuk BSSN agar dapat mengenali risiko dari keamanan informasi khususnya pada sektor Pendidikan.
- BSSN dapat menindaklanjuti dengan merumuskan kebijakan maupun kegiatan untuk meminimalisir risiko yang telah teridentifikasi.
- Parameter penilaian merupakan parameter yang dibuat oleh BSSN, dan tidak menggambarkan dampak dan probabilitas dari masing-masing responden atau referensi yang dijadikan acuan oleh *stakeholder*.

Pernyataan Kerahasiaan

Segala informasi yang anda sampaikan pada survei ini bersifat **RAHASIA** dan disimpan pada Drive BSSN dengan aman serta hanya diolah dan didistribusikan kepada pihak Internal BSSN terkait.

INFORMASI RESPONDEN
(Mohon diisi oleh Penanggung Jawab IT)

1. Nama Organisasi :
2. *Website* Organisasi :
3. Alamat Email Organisasi :
4. No. Telp Organisasi :
5. Nama Responden :
6. Email Responden :
7. No. HP/WA Responden :
8. Jabatan :

DAFTAR ISTILAH

1. **Kritikal** adalah status dari Aset Informasi yang apabila aspek keamanannya terganggu, maka akan berdampak signifikan bagi kelangsungan aktifitas bisnis Organisasi. Aspek keamanan sebagaimana dimaksud, meliputi: *confidentiality* (kerahasiaan), *integrity* (keutuhan), dan/atau *availability* (ketersediaan).
2. *Business Continuity Planning* (BCP) adalah sebuah strategi untuk mengatasi keadaan dimana kondisi bisnis harus dapat terus berjalan pasca terjadinya bencana.
3. *Disaster recovery planning* (DRP) adalah perencanaan untuk pengelolaan secara rasional dan biaya efektif bencana terhadap sistem informasi yang akan dan telah terjadi.
4. *Disaster Recovery System* (DRC) adalah suatu tempat khusus untuk menempatkan sistem, aplikasi, hingga data-data cadangan organisasi/perusahaan ketika terjadi gangguan serius atau bencana yang menimpa satu atau berbagai unit kerja di organisasi/perusahaan, seperti pusat penyimpanan dan pengolahan data dan informasi.
5. *Intrusion Detection System* (IDS) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan.
6. *Intrusion Prevention System* (IPS) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan serta melakukan pencegahan dini terhadap intrusi atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya.
7. *Remote Learning System* merupakan sistem pembelajaran jarak jauh di mana siswa (peserta pelatihan) dan pendidik, tidak hadir secara fisik di kelas tradisional atau tatap muka. Pembelajaran atau transfer informasi disampaikan dengan melibatkan teknologi, seperti konferensi video dan penilaian daring (*online*).
8. *IOT (Internet of Things)* merupakan suatu jaringan fisik yang dipasang pada sensor, software dan teknologi lain dengan tujuan agar bisa terhubung dan bertukar data antar perangkat dan sistem lain dengan menggunakan internet.
9. *Social Engineering Attack* merupakan sebuah teknik manipulasi yang memanfaatkan kesalahan manusia untuk mendapatkan akses pada informasi pribadi atau data-data berharga.
10. *Denial of Service* merupakan serangan di mana pelaku berupaya membuat mesin atau sumber daya jaringan tidak tersedia bagi pengguna yang dituju dengan mengganggu layanan host yang terhubung ke Internet untuk sementara atau tanpa batas.

BAB I

PENDAHULUAN

Deskripsi Permasalahan

Berdasarkan Lanskap Keamanan Siber Indonesia Tahun 2023 yang dirilis oleh Badan Siber dan Sandi Negara (BSSN), terdapat beberapa ancaman yang telah menyebabkan insiden maupun yang berpotensi menjadi insiden seperti *ransomware*, *phishing*, *data breach*, dan *web defacement* (khususnya penyusupan iklan perjudian dalam jaringan). Data ini diperoleh baik dari hasil pemantauan tim BSSN maupun laporan aduan dari *stakeholder*. Ancaman tersebut telah mengakibatkan dampak yang mempengaruhi *stakeholder* dari berbagai sektor, termasuk sektor Pendidikan. Hal ini menjadi risiko yang perlu dilakukan pengendalian atau mitigasi untuk mengurangi dampak yang ditimbulkan.

1. *Ransomware*

Ransomware adalah jenis malware yang digunakan untuk menyandera aset korban, seperti dokumen, sistem, ataupun perangkat. Setelah aset terenkripsi, korban akan diminta membayar tebusan untuk mendekripsi dan kembali mendapatkan akses pada aset. *Ransomware* menargetkan individu, perusahaan, organisasi, bahkan Pemerintah. Dampak *ransomware* dapat berupa kehilangan akses terhadap data, kerugian finansial, hingga penurunan reputasi. Pada tahun 2023, BSSN mencatat terdapat 1.011.209 aktivitas *ransomware* yang terdeteksi.

2. *Phishing*

Phishing adalah upaya untuk memperoleh informasi pribadi seperti *password* dan rincian keuangan dengan menyamar sebagai entitas terpercaya melalui komunikasi elektronik, sering kali melalui *email* atau situs web palsu. Serangan *phishing* termasuk dalam jenis serangan yang perlu menjadi fokus berdasarkan banyaknya masyarakat yang menjadi korban. *Phishing* juga termasuk ke dalam 10 besar insiden yang terjadi tahun 2023 berdasarkan data penanganan insiden BSSN. Pada tahun 2024, diperkirakan akan banyak terjadi serangan *phishing* tingkat lanjut.

3. *Data Breach*

Kejadian kebocoran data (*data breach*) merupakan situasi dalam ruang siber di mana informasi atau data rahasia yang dimiliki oleh suatu organisasi diakses dan diungkap kepada publik oleh pihak yang mengancam, tanpa sepengetahuan pemilik sistem. Data yang diambil oleh *threat actor* biasanya termasuk informasi yang bersifat sangat pribadi, seperti *Personal Identifiable Information* (PII), data yang sangat rahasia bagi individu maupun organisasi, dan informasi lainnya yang semestinya hanya diketahui oleh pihak yang berwenang. Berdasarkan hasil pemantauan dan analisis *Cyber Threat Intelligence*, BSSN telah melakukan penelusuran dugaan insiden siber dengan jumlah total 347 dugaan insiden siber dengan jumlah jenis dugaan insiden tertinggi yaitu *Data Breach*. Hasil penelusuran pada *darknet*, ditemukan adanya 1.674.185 temuan *data exposure* yang berdampak pada 429 *stakeholder* di Indonesia.

4. *Web Defacement*

Ancaman *web defacement* merupakan bentuk serangan siber yang mengubah tampilan suatu situs web dengan tujuan menyampaikan pesan atau merusak reputasi pemiliknya. Pada sebuah serangan *web defacement*, *threat actor* seringkali memilih target yang memiliki nilai simbolis, seperti situs web pemerintah, perusahaan besar, atau lembaga penting. Pesan yang disampaikan bervariasi, mulai dari pesan teks, gambar, hingga pesan politis atau ideologis. *Threat actor* seringkali memanfaatkan celah keamanan pada situs web atau menggunakan teknik *hacking* untuk mendapatkan akses tak sah, sehingga dapat dengan mudah mengganti halaman utama situs tersebut dengan pesan atau konten yang dimaksudkan. Ancaman *web defacement* tidak hanya merupakan pelanggaran terhadap privasi dan integritas suatu situs web, tetapi juga dapat memiliki dampak serius terhadap reputasi dan kepercayaan pengguna yang mengakses situs tersebut. Pada kasus *web defacement* ditemukan sebanyak 189 kasus yang telah dinotifikasi oleh BSSN dengan klasifikasi kasus paling banyak adalah *web defacement* pada halaman tersembunyi (*hidden*).

BAB II

PENERAPAN KONTROL KEAMANAN INFORMASI

Deskripsi

Bab ini bertujuan untuk memotret potensi risiko keamanan informasi di lingkungan organisasi berdasarkan ancaman *ransomware*, *data breach*, *web defacement* dan *phishing*. Komponen yang digunakan didasari oleh taktik, teknik dan prosedur yang umumnya digunakan oleh *threat actor*. Adapun acuan yang digunakan berdasarkan MITRE ATT&CK dengan variabel sebagai berikut:

1. *Application Developer Guidance*
2. *User Account Management*
3. *Multi-factor Authentication*
4. *Password Policies*
5. *User Training*
6. *Restrict Web-Based Content*
7. *Restrict File and Directory*
8. *Privileged Account Management*
9. *Network Segmentation*
10. *Network Intrusion Prevention*
11. *Limit Access to Resource Over Network*
12. *Account Use Policies*
13. *Execution Prevention*
14. *Disable or Remove Feature or Program*
15. *Audit*
16. *Vulnerability Scanning*
17. *Antivirus/Antimalware*
18. *Exploit Protection*
19. *Update Software*
20. *Data Backup*
21. *Encrypt Sensitive Information*
22. *Remote Data Storage*
23. *Software Configuration*
24. *Data Loss Prevention*

Kuesioner ini tidak menggunakan kontrol mitigasi MITRE ATT&CK secara menyeluruh dan bukan merupakan acuan mitigasi keamanan secara ideal. Pemilihan kontrol mitigasi dalam kuesioner ini adalah berdasarkan hal-hal yang menjadi penyebab pada sebagian besar insiden *ransomware*, *phishing*, *data breach* dan *web defacement*. Dengan fokus ini diharapkan dapat tertangkap kondisi aktual pada responden yang kemudian data dari hasil survei ini dapat dijadikan acuan dalam merencanakan program, inisiatif prioritas maupun strategi keamanan siber.

Petunjuk Pengisian

Berilah tanda centang (✓) pada kolom yang tersedia untuk setiap pernyataan yang sesuai dengan kondisi di organisasi Anda. Responden diperbolehkan memberi lebih dari satu tanda centang untuk setiap aspek. Centang pada kolom tidak, apabila tidak terdapat pernyataan yang sesuai pada penerapan organisasi.

Aspek 1. Application Developer Guidance

Dalam melakukan pengembangan aplikasi, manakah diantara hal-hal berikut ini yang telah diatur dan dijalankan oleh organisasi?

No	Pernyataan	Ya	Tidak
1.1	Penggunaan <i>library</i> pihak ketiga yang tepercaya	☐	☐

Aspek 2. User Account Management

Organisasi memastikan keamanan pengelolaan akun dengan cara:

No	Pernyataan	Ya	Tidak
2.1	Menerapkan dan memastikan prinsip <i>least privilege</i> pada <i>control access</i>	☐	☐
2.2	Membatasi <i>privilege</i> akun dan grup pengguna sehingga hanya administrator resmi yang dapat berinteraksi dengan perubahan layanan dan konfigurasi layanan.	☐	☐

Least Privilege adalah konsep yang menyatakan bahwa pengguna hanya memiliki akses terhadap apa yang menjadi kewenangannya sesuai tugas dan fungsinya.

Aspek 3. Multi-factor Authentication (MFA)

Penerapan MFA memperhatikan hal-hal sebagai berikut:

No	Pernyataan	Ya	Tidak
3.1	Organisasi menerapkan MFA yaitu menggunakan 2 (dua) atau lebih parameter untuk otentikasi?	☐	☐

Aspek 4. Password Policies

Organisasi menerapkan kebijakan *password* aman dengan kriteria sebagai berikut

No	Pernyataan	Ya	Tidak
4.1	Mensyaratkan penerapan kebijakan <i>password</i> aman (batas panjang minimal <i>password</i> , kombinasi <i>password</i> , penggantian <i>password</i> berkala, dst)	☐	☐

Aspek 5. User Training (Security Awareness)

Organisasi menyelenggarakan program untuk meningkatkan kesadaran dan pemahaman keamanan informasi kepada para Pegawai tentang hal-hal sebagai berikut

No	Pernyataan	Ya	Tidak
5.1	Ancaman <i>phishing</i> melalui <i>attachment</i> , <i>link</i> , <i>service</i> , <i>voice</i> dan langkah-langkah pencegahannya.	☐	☐
5.2	Mekanisme pelaporan oleh Pegawai apabila mendapati upaya <i>phishing</i> .	☐	☐

Aspek 6. Restrict Web-Based Content

Organisasi melakukan pembatasan terhadap konten pada situs dengan melakukan hal-hal, sebagai berikut?

No	Pernyataan	Ya	Tidak
6.1	Memblokir akses terhadap media sosial, <i>email</i> pribadi, atau layanan lain yang dapat menimbulkan risiko signifikan seperti <i>phishing</i> .	☐	☐
6.2	Menjalankan prosedur pemblokiran terhadap lampiran-lampiran tidak dikenal yang tidak umum dikirimkan melalui <i>email</i> (contoh: *.scr, *.exe, *.pif, *.cpl.)	☐	☐

Aspek 7. Restrict File and Directory Permissions

Organisasi melakukan pembatasan izin pada file dan direktori dengan rincian sebagai berikut:

No	Pernyataan	Ya	Tidak
7.1	Membatasi berbagi file ke direktori tertentu dengan akses yang hanya diperlukan.	☐	☐

Aspek 8. Privileged Account Management

Organisasi mengelola akun *privilege* dengan melakukan hal-hal, sebagai berikut

No	Pernyataan	Ya	Tidak
8.1	Melakukan audit domain dan akun lokal serta level izinnya masing-masing secara rutin	☐	☐
8.2	Tidak mengizinkan penggunaan akun pada domain administrator di luar keperluan administratif	☐	☐

Aspek 9. Network Segmentation

Organisasi menerapkan segmentasi jaringan, dengan cara:

No	Pernyataan	Ya	Tidak
9.1	Menerapkan praktik terbaik dalam mengonfigurasi <i>firewall</i> untuk memastikan hanya port dan trafik yang diperlukan untuk dapat keluar dan masuk jaringan	☐	☐
9.2	Menerapkan segmentasi server dan layanan yang terekspos ke publik dengan <i>Demilitarized Zone</i> (DMZ) atau pada infrastruktur hosting terpisah	☐	☐

Aspek 10. Network Intrusion Prevention

Organisasi menerapkan teknologi pendeteksi dan pencegah intrusi pada jaringan dengan cara:

No	Pernyataan	Ya	Tidak
10.1	Mengoptimalkan fungsi perangkat untuk mendeteksi dan mencegah percobaan serangan terhadap aplikasi dan jaringan	☐	☐

Aspek 11. Limit Access to Resource Over Network

No	Pernyataan	Ya	Tidak
11.1	Organisasi membatasi akses ke sumber daya jarak jauh	☐	☐

Aspek 12. Account Use Policies

Organisasi menerapkan kebijakan penggunaan akun untuk memastikan hal-hal sebagai berikut:

No	Pernyataan	Ya	Tidak
12.1	Mengunci akun secara otomatis setelah serangkaian percobaan login yang gagal	☐	☐

Aspek 13. Execution Prevention

Organisasi mengembangkan kemampuan dalam melakukan pengendalian terhadap eksekusi aplikasi melalui hal-hal, sebagai berikut:

No	Pernyataan	Ya	Tidak
13.1	Menerapkan <i>allow listing</i> untuk memastikan hanya aplikasi yang diizinkan yang boleh dijalankan	☐	☐

Aspek 14. Disable or Remove Feature or Program

Organisasi memastikan keamanan fitur atau program dengan melakukan hal-hal, sebagai berikut:

No	Pernyataan	Ya	Tidak
14.1	Menutup seluruh port dan layanan yang tidak digunakan	☐	☐

Aspek 15. Audit

Organisasi melakukan audit dengan rincian, sebagai berikut:

No	Pernyataan	Ya	Tidak
15.1	Melakukan audit atau pemindaian terhadap sistem, izin, perangkat lunak, konfigurasi untuk menemukan kerentanan	☐	☐

Aspek 16. Vulnerability Scanning

Untuk melakukan penemuan kerentanan aplikasi, maka organisasi melaksanakan hal-hal sebagai berikut:

No	Pernyataan	Ya	Tidak
16.1	Melakukan pemindaian kerentanan dan <i>code review</i> berkala terhadap aplikasi-aplikasi yang dapat diakses dari internet	☐	☐
16.2	Menyediakan saluran komunikasi untuk mengakomodir aduan atau laporan publik tentang pengungkapan kerentanan pada aplikasi organisasi	☐	☐
16.3	Melakukan remediasi terhadap kerentanan-kerentanan yang telah tervalidasi	☐	☐

Aspek 17. Antivirus/Antimalware

No	Pernyataan	Ya	Tidak
17.1	Organisasi mensyaratkan penggunaan <i>antivirus</i> / <i>antimalware</i>	☐	☐

Aspek 18. Exploit Protection

Organisasi menerapkan sistem proteksi dari upaya eksploitasi dengan melakukan hal-hal, sebagai berikut:

No	Pernyataan	Ya	Tidak
18.1	Menerapkan <i>web application firewall</i> (WAF)	☐	☐

Aspek 19. Update Software

Organisasi memastikan pemutakhiran perangkat lunak dengan cara, sebagai berikut:

No	Pernyataan	Ya	Tidak
19.1	Menerapkan <i>patch management</i>	☐	☐

Aspek 20. Data Backup

Organisasi menjalankan fungsi pencadangan data dengan:

No	Pernyataan	Ya	Tidak
20.1	Menerapkan rencana pemulihan bencana TI yang berisi prosedur untuk mengambil dan menguji cadangan data secara berkala.	☐	☐
20.2	Data cadangan disimpan di luar sistem dan terlindungi dari ancaman penyerang.	☐	☐

Aspek 21. Encrypt Sensitive Information

Organisasi menjamin kerahasiaan data/informasi sensitif dengan enkripsi dengan rincian, sebagai berikut:

No	Pernyataan	Ya	Tidak
21.1	Mengenkripsi data/informasi penting organisasi	☐	☐

Aspek 22. Remote Data Storage

Organisasi melakukan penyimpanan data jarak jauh secara aman dengan melakukan hal-hal, sebagai berikut:

No	Pernyataan	Ya	Tidak
22.1	Melakukan penerusan catatan kejadian (<i>event</i>) ke dalam <i>log server</i> atau repositori data secara otomatis	☐	☐

Aspek 23. Software Configuration

Organisasi memastikan penerapan konfigurasi perangkat lunak dengan memperhatikan hal-hal, sebagai berikut:

No	Pernyataan	Ya	Tidak
23.1	Menerapkan mekanisme autentikasi email dan anti-spoofing menggunakan <i>Sender Policy Framework</i> (SPF) dan <i>DomainKeys Identified Mail</i> (DKIM)	☐	☐

Aspek 24. Data Loss Prevention

No	Pernyataan	Ya	Tidak
24.1	Organisasi menerapkan perangkat <i>Data Loss Prevention</i> (DLP)	☐	☐

BAB III

ANATOMI KEAMANAN INFORMASI

Deskripsi

Pada bagian ini Responden akan diberikan sejumlah pertanyaan mengenai anatomi keamanan informasi yang digunakan / dikelola oleh Organisasi dalam menjalankan aktifitas layanan.

Petunjuk Pengisian

Mohon untuk mengisi kuesioner berikut sesuai dengan kondisi saat ini di Organisasi Anda;

Pertanyaan

1. Aspek Tata Kelola

- a. Apakah organisasi anda memiliki kebijakan Sistem Manajemen Keamanan Informasi?
 - ☐ Ya
 - ☐ Tidak
- b. Apakah organisasi anda memiliki kebijakan manajemen risiko?
 - ☐ Ya
 - ☐ Tidak
- c. Apakah organisasi anda memiliki kebijakan manajemen aset?
 - ☐ Ya
 - ☐ Tidak
- d. Apakah organisasi anda memiliki kebijakan DRP?
 - ☐ Ya
 - ☐ Tidak
- e. Apakah organisasi anda memiliki kebijakan BCP?
 - ☐ Ya
 - ☐ Tidak

2. Aspek Teknologi & Operasi

- a. Apakah anda memiliki DC (Data Center)?
 - ☐ Ya
 - ☐ Tidak
 1. Apakah DC dilakukan secara on-premis atau menggunakan cloud?
 - ☐ On-premis
 - ☐ Cloud
 2. Apakah DC dikelola secara mandiri atau melalui pihak ke-3?
 - ☐ Mandiri
 - ☐ Pihak ke-3
- b. Apakah anda memiliki DRC (*Disaster Recovery System*)?
 - ☐ Ya
 - ☐ Tidak

1. Apakah DRC dilakukan secara on-premis atau menggunakan cloud?
 - On-premise
 - Cloud
- c. Sistem Elektronik
Sebutkan Sistem Elektronik yang anda kelola?

No	Nama Sistem Elektronik	Deskripsi	Status Vital

3. Aspek Sumber Daya Manusia

- a. Berapakah jumlah sumber daya manusia (SDM) yang ditugaskan untuk menangani bidang keamanan informasi dan keamanan siber di lingkungan organisasi?
- b. Apakah personel yang mempunyai tugas dan tanggung jawab terkait teknologi informasi (TI) pernah mengikuti pelatihan di bidang Keamanan Informasi dan atau Keamanan Siber? Jika “Ya” Sebutkan!

- Ya

No.	Nama	Jabatan	Pelatihan

- Tidak

- c. Apakah personel yang mempunyai tugas dan tanggung jawab terkait teknologi informasi (TI) memiliki sertifikat kompetensi di bidang Keamanan Informasi dan atau Keamanan Siber? Jika “Ya” Sebutkan!

- Ya

No.	Nama	Jabatan	Sertifikasi

- Tidak

4. Aspek Keberlanjutan Organisasi dan Pengelolaan Krisis

- a. Apakah organisasi anda terdapat prosedur penanganan insiden siber?
 - Ya
 - Tidak
- b. Apakah organisasi Anda telah membuat laporan insiden untuk setiap insiden siber dan dilaporkan ke *top management*?
 - Ya
 - Tidak
- c. Apakah organisasi anda memiliki CSIRT?
 - Ya
 - Tidak

5. Aspek Kepatuhan

- a. Apakah pernah dilakukan asesmen/pengujian terkait Keamanan Teknologi Informasi baik dari segi teknis maupun tata kelola (Contoh: IT Security Assessment, Audit SNI ISO/IEC 27001, Asesmen Indeks KAMI)?
 - Sudah, baik Internal maupun Eksternal
 - Sudah, hanya Internal
 - Tidak dilakukan
- b. Apakah telah dilakukan sertifikasi ISO 27001?
 - Ya
 - Tidak

BAB IV

ASET ORGANISASI

Deskripsi

Pada bagian ini Responden akan diberikan sejumlah pertanyaan mengenai aset yang dimiliki / dikelola oleh Organisasi dalam menjalankan aktivitas layanan.

Petunjuk Pengisian

Mohon untuk mengisi kuesioner berikut sesuai dengan kondisi saat ini di Organisasi Anda;

Pertanyaan

1. Terkait aset *endpoint devices* atau perangkat Organisasi
 - a. Apakah organisasi Anda mengizinkan pegawai/karyawan menyimpan data sensitif organisasi pada perangkat pribadi?
 - ☐ Ya
 - ☐ Tidak
2. Terkait aset bangunan (*Buildings*)
 - a. Apakah fasilitas pemrosesan data/informasi di Organisasi dilengkapi sumber daya listrik cadangan?
 - ☐ Ya
 - ☐ Tidak
 - b. Apakah fasilitas pemrosesan data/informasi (ruang server) di Organisasi telah dilengkapi dengan akses kontrol (misal: kunci akses dengan biometri)?
 - ☐ Ya
 - ☐ Tidak
 - c. Apakah fasilitas pemrosesan data/informasi di Organisasi telah dilengkapi dengan CCTV?
 - ☐ Ya
 - ☐ Tidak
 - d. Apakah fasilitas pemrosesan data/informasi di Organisasi telah dilengkapi dengan sistem pendeteksi dan pemadam kebakaran?
 - ☐ Ya
 - ☐ Tidak