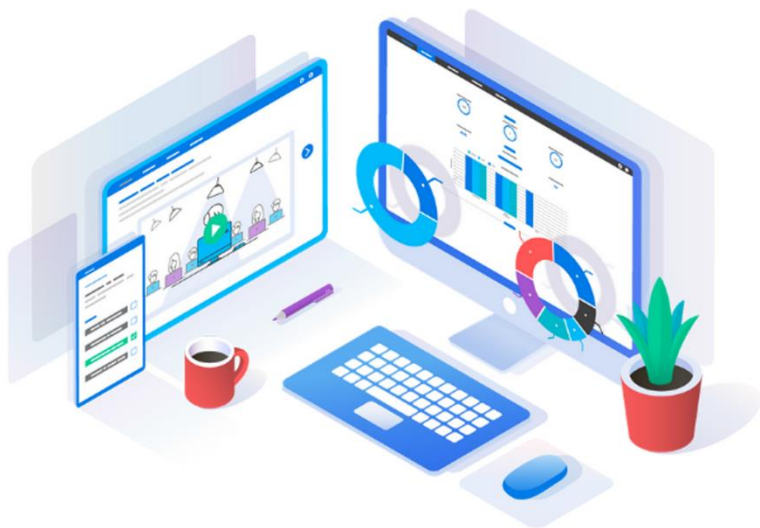




# PENILAIAN MANDIRI KEAMANAN INFORMASI (PAMAN KAMI)

UNTUK USAHA KECIL MENENGAH

EDISI BAHASA INDONESIA



**Gunakan -PAMAN KAMI-** untuk memeriksa  
status keamanan informasi usaha Anda

**Lindungi aset usaha Anda !**

# **Penilaian Mandiri Keamanan Informasi (PAMAN KAMI) Untuk Usaha Kecil Menengah**



# Penilaian Mandiri Keamanan Informasi (PAMAN KAMI) Untuk Usaha Kecil Menengah

Diterbitkan oleh  
Badan Siber dan Sandi Negara, 2020.  
Jalan Harsono RM No. 70  
Ragunan, Pasar Minggu  
Jakarta Selatan 12550  
[www.bssn.go.id](http://www.bssn.go.id)

Cetakan Pertama: Februari 2020

## *Susunan Redaksi*

Pembina : Akhmad Toha, S.AP.  
Pengarah : Anton Setiyawan, S.Si., M.M.  
Penyusun : Baderi, S.Sos., M.E., C.CISO.  
Eko Tulus Budi Cahyanto, S.S.T.TP.

Penilaian Mandiri Keamanan Informasi  
(PAMAN KAMI) Untuk Usaha Kecil Menengah  
**Badan Siber dan Sandi Negara,**  
Jakarta; BSSN; 2020  
36 hlm; 14,8 x 21 cm  
ISBN: 978-623-93005-0-0

Hak Cipta dilindungi Undang-Undang Republik Indonesia Nomor 28 Tahun 2014  
tentang Hak Cipta



## Kata Pengantar



### ***Salam Aman dan Sejahtera bagi kita semua,***

Indonesia telah memasuki babak baru dalam era yang serba siber, yang ditandai dengan hadirnya revolusi industri 4.0. Hal tersebut menuntut Pemerintah, masyarakat, dan dunia usaha untuk dapat beradaptasi dengan perkembangan siber.

Interaksi sosial masyarakat turut berubah seiring hadirnya teknologi siber yang menyediakan berbagai macam kemudahan dalam bertransaksi. Dunia usaha tradisional atau konvensional dalam bentuk usaha mikro, kecil maupun menengah mengalami pergeseran menuju era baru dengan memanfaatkan media siber seperti media sosial, mesin pencari (*search engine*), *website*, dan *platform marketplace* dalam menjalankan usahanya. Usaha dengan memanfaatkan media siber sangat mempermudah masyarakat karena dapat mengefisienkan waktu, tempat, dan biaya.

Di sisi lain, kemajuan teknologi siber tersebut ternyata memiliki dampak negatif pada kegiatan usaha. Semakin berkembangnya teknologi siber, maka akan semakin berkembang pula jenis kejahatan baru. Kejahatan yang dimaksud dikenal dengan nama kejahatan siber. Kejahatan siber ini menyerang unsur-unsur dunia siber, yang salah satunya menasar pada usaha yang memanfaatkan media digital. Kejahatan siber tersebut dapat mengakibatkan timbulnya kerugian bagi para pelaku atau pemilik usaha, mulai dari kerugian reputasi hingga kerugian finansial.

Guna mencegah terjadinya kerugian tersebut sejak dini, maka diperlukan langkah proteksi yang dimulai dari pemahaman akan pentingnya keamanan siber (keamanan informasi). Dengan adanya pemahaman akan pentingnya keamanan siber, para pelaku usaha diharapkan mampu menerapkan prinsip-prinsip keamanan siber dalam membangun dan mengembangkan usahanya, sehingga dapat berjalan dengan aman dan lancar.

Menyikapi permasalahan tersebut, Badan Siber dan Sandi Negara Republik Indonesia (BSSN) mempersembahkan pedoman **Penilaian Mandiri Keamanan Informasi Untuk Usaha Kecil Menengah** yang selanjutnya disebut **PAMAN KAMI untuk UKM**. PAMAN KAMI sebagai solusi praktis yang kami tawarkan bagi UKM di seluruh Indonesia, bahkan tidak menutup kemungkinan ditawarkan kepada



masyarakat dunia melalui forum-forum ekonomi internasional. Kami berharap PAMAN KAMI dapat digunakan oleh pelaku UKM sebagai langkah awal guna memeriksa status keamanan informasi di usahanya, sehingga dapat mencegah maupun menanggulangi terjadinya insiden serangan siber. Inilah bentuk peran serta BSSN dalam mewujudkan keamanan nasional serta meningkatkan pertumbuhan perekonomian nasional.

Demikian persembahan kami, apresiasi dan terima kasih disampaikan untuk semua pihak yang telah berperan dalam penyusunan dan para pengguna pedoman PAMAN KAMI untuk UKM.

***Bersama BSSN, Kita Aman dan Sejahtera***

Jakarta, 22 Januari 2020

Kepala Badan Siber dan Sandi Negara,

ttd.

Letjen TNI (Purn) Hinsu Siburian



Daftar Isi

Kata Pengantar ..... 3

Daftar Isi ..... 5

PAMAN KAMI untuk UKM ..... 6

Penjelasan Kerentanan dan Langkah Proteksi ..... 13

Referensi ..... 34

Riwayat Perubahan Pra Launching ..... 35



## PAMAN KAMI untuk UKM

**PAMAN KAMI** fokus pada 25 langkah keamanan informasi bagi pelaku UKM. Pengisian PAMAN KAMI membutuhkan waktu kurang lebih 5 menit dan dapat diterapkan dengan biaya yang minim. **PAMAN KAMI** dapat digunakan sebagai langkah awal untuk mengukur tingkat keamanan informasi pada pelaku UKM sehingga insiden serangan siber dapat dicegah dan diminimalisasi dengan lebih baik. Di samping itu, para pelaku UKM dapat membangun dan mengembangkan usahanya dengan lancar dan aman dari serangan siber demi mewujudkan keamanan nasional serta meningkatkan pertumbuhan perekonomian nasional.

Langkah keamanan informasi pada **PAMAN KAMI** bisa digunakan dengan syarat sebagai berikut:

- ❖ Organisasi usaha tidak memiliki server atau peralatan jaringan yang memerlukan pengaturan rumit.
- ❖ Tidak ada perangkat lunak aplikasi yang dikembangkan secara mandiri oleh organisasi usaha, dan hanya menggunakan perangkat lunak aplikasi/*platform* yang tersedia secara komersial/pihak ketiga.

|                                                                |                                                                                                                                      |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Jika Anda mencetak 100 poin<br><b>(SEMPURNA)</b>               | Langkah keamanan informasi yang Anda terapkan sudah sempurna. Rencanakan langkah untuk naik ke level berikutnya.                     |
| Jika Anda mencetak 90-99 poin<br><b>(BAIK)</b>                 | Hampir sempurna, namun ada beberapa langkah yang belum diterapkan secara menyeluruh, sehingga butuh penerapan keamanan lebih lanjut. |
| Jika Anda mencetak 70-89 poin<br><b>(CUKUP)</b>                | Langkah keamanan cukup baik. Terapkan langkah proteksi yang ada untuk meningkatkan keamanan informasi Anda.                          |
| Jika Anda mencetak 50 - 69 poin<br><b>(KURANG)</b>             | Terdapat bidang yang secara eksplisit mengalami kekurangan langkah keamanan.                                                         |
| Jika Anda mencetak 49 poin atau lebih rendah<br><b>(BURUK)</b> | Keamanan informasi perusahaan Anda buruk. Anda seharusnya tidak terkejut jika terjadi insiden seperti kebocoran data.                |

## Petunjuk Pengisian

- Jawablah seluruh pertanyaan dibawah ini dengan jujur.
- Berilah tanda (x) pada kolom yang tersedia dan pilih sesuai dengan keadaan yang sebenarnya.

### Identitas Usaha (Perusahaan)

Nama Usaha : \_\_\_\_\_

Branding : \_\_\_\_\_

Skala Usaha : ☐ Mikro ☐ Kecil ☐ Menengah

Bentuk Usaha : ☐ Firma ☐ CV ☐ PT

☐ Koperasi ☐ Perseorangan

☐ Lainnya Sebutkan: \_\_\_\_\_

Aset Usaha : ☐ < 50 jt ☐ 50 - 500 jt ☐ 50 jt – 10 M

☐ > 50 M

Omzet Usaha : ☐ < 300 jt ☐ 300 jt - 2,5 M ☐ 2,5 M – 50 M

☐ > 50 M

Karyawan : ☐ < 10 Orang ☐ 11 - 30 Orang ☐ 30 – 300 Orang

☐ >300 Orang

Alamat : \_\_\_\_\_

## Media Digital Usaha

Media Sosial : ☐ Facebook ☐ Instagram ☐ Line  
☐ Lainnya *Sebutkan:* \_\_\_\_\_

Marketplace : ☐ Bukalapak ☐ Shopee ☐ Blibli ☐ Bhineka  
☐ Tokopedia ☐ Lazada ☐ JD.ID ☐ Zalora  
☐ Lainnya *Sebutkan:* \_\_\_\_\_

Website Pribadi : \_\_\_\_\_

Mobile Apps : \_\_\_\_\_

## Identitas Pemilik Usaha atau Pengisi PAMAN KAMI

Nama : \_\_\_\_\_

Jabatan : \_\_\_\_\_

No HP : \_\_\_\_\_

Email : \_\_\_\_\_

Jenis Kelamin : ☐ Laki - Laki ☐ Perempuan

Pendidikan : ☐ SD ☐ SMP ☐ SMA ☐ D3  
☐ D4/S1 ☐ S2 ☐ S3

Umur : ☐ < 20 th ☐ 20–30 th ☐ 30–40 th ☐ 40–50 th  
☐ >50 th

### Petunjuk Pengisian **PAMAN KAMI Versi 2.0**

- Bacalah item pertanyaan penilaian di bawah ini dan pilih kolom yang sesuai dengan kondisi penerapan keamanan informasi pada usaha (perusahaan) Anda.
- Penilaian ini diprioritaskan diisi oleh pimpinan atau manajer usaha (perusahaan).
- Pimpinan atau manajer usaha (perusahaan) dapat secara langsung menginstruksikan dan mengonfirmasi kepada bagian terkait, apakah langkah kebijakan keamanan telah diimplementasikan.
- Jawablah apakah item pertanyaan penilaian nomor 1 s.d. 25 telah diterapkan oleh usaha (perusahaan) Anda dan silakan pilih:
  - ❖ **DM (Diterapkan Menyeluruh)**, jika item penilaian diterapkan secara menyeluruh terhadap seluruh karyawan baik pribadi maupun organisasi.
  - ❖ **DS (Diterapkan Sebagian)**, jika item penilaian hanya diterapkan oleh sebagian dari karyawan atau organisasi.
  - ❖ **TD (Tidak Diterapkan)**, jika item penilaian belum diterapkan sama sekali oleh karyawan maupun organisasi.
  - ❖ **TT (Tidak Tahu)**, jika Anda belum memahami item penilaian tersebut.

| NO | ITEM PERTANYAAN PENILAIAN                                                                                                             | PENERAPAN |    |    |    |
|----|---------------------------------------------------------------------------------------------------------------------------------------|-----------|----|----|----|
|    |                                                                                                                                       | DM        | DS | TD | TT |
| 1  | Apakah Anda sudah melakukan identifikasi terhadap aset-aset penting usaha (perusahaan) yang harus dilindungi?                         | 4         | 2  | 0  | 0  |
| 2  | Apakah Anda sudah melakukan identifikasi terhadap semua kemungkinan risiko hilangnya aset-aset penting usaha (perusahaan)?            | 4         | 2  | 0  | 0  |
| 3  | Apakah Anda memiliki prosedur dan kebijakan keamanan informasi yang diterapkan untuk melindungi aset-aset penting usaha (perusahaan)? | 4         | 2  | 0  | 0  |

|    |                                                                                                                                                                                                                                                                            |   |   |   |   |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---|
| 4  | Apakah Anda menerapkan penggunaan kata sandi ( <i>password</i> ) pada perangkat komputer, laptop dan/atau <i>smartphone</i> untuk mencegah pencurian data?                                                                                                                 | 4 | 2 | 0 | 0 |
| 5  | Sudahkah Anda membuat kata sandi ( <i>password</i> ) yang kuat dan tidak mudah ditebak serta tidak menggunakan kata sandi yang sama untuk beberapa Akun (layanan web)?                                                                                                     | 4 | 2 | 0 | 0 |
| 6  | Apakah Anda menerapkan langkah untuk mencegah hilang atau bocornya informasi penting, seperti menyimpan informasi penting di kabinet/lemari/laci yang terkunci, dan tidak meninggalkannya di atas meja?                                                                    | 4 | 2 | 0 | 0 |
| 7  | Saat melihat ada orang yang tidak dikenal memasuki area kerja terbatas milik usaha (perusahaan), apakah Anda melakukan pengamanan dengan cara mendekati dan menanyakan maksud dan tujuan kedatangan orang tersebut?                                                        | 4 | 2 | 0 | 0 |
| 8  | Apakah Anda sudah memasang alat elektronik anti petir ( <i>Surge Protector</i> ) dan <i>Uninterruptible Power Supplies</i> (UPS) yang digunakan untuk melindungi perangkat jaringan usaha (perusahaan) dari sambaran petir, lonjakan listrik atau hubungan pendek listrik? | 4 | 2 | 0 | 0 |
| 9  | Saat membuang/menghapus informasi penting, apakah Anda sudah memastikan bahwa informasi penting yang dibuang/dihapus menjadi tidak terbaca lagi, seperti menggunakan penghancur kertas/alat penghapus data?                                                                | 4 | 2 | 0 | 0 |
| 10 | Apakah Anda menerapkan kebijakan tidak menghubungkan komputer, laptop, dan <i>smartphone</i> Anda dengan jaringan internet (Wi-Fi) publik pada saat mengakses akun-akun penting?                                                                                           | 4 | 2 | 0 | 0 |

|    |                                                                                                                                                                                                                                                                         |   |   |   |   |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---|
| 11 | Apakah Anda menerapkan cara untuk menghindari serangan rekayasa sosial ( <i>social engineering</i> ) seperti membatasi informasi pribadi yang dibagikan kepada publik atau bersikap skeptis terhadap orang tidak dikenal yang ingin mengetahui informasi sensitif Anda? | 4 | 2 | 0 | 0 |
| 12 | Apakah Anda selalu menjaga <i>Operating System</i> , <i>smartphone</i> , perangkat lunak dan aplikasi usaha (perusahaan) mendapatkan pembaruan ( <i>update</i> ) keamanan dari vendor/penyedia secara otomatis?                                                         | 4 | 2 | 0 | 0 |
| 13 | Apakah Anda selalu memastikan bahwa aplikasi yang Anda unduh dan instal pada komputer, laptop, dan <i>smartphone</i> usaha (perusahaan) aman dan berasal dari sumber tepercaya?                                                                                         | 4 | 2 | 0 | 0 |
| 14 | Apakah Anda menerapkan kebijakan untuk mengontrol penggunaan Internet, seperti menetapkan aturan tentang menjelajahi situs web dan mengunggah ke media sosial di komputer area kerja (kantor)?                                                                          | 4 | 2 | 0 | 0 |
| 15 | Apakah Anda mempunyai program untuk memberikan pemahaman kepada karyawan akan pentingnya keamanan informasi dan bahwa keamanan informasi merupakan tanggung jawab semua orang yang bekerja pada usaha (perusahaan) Anda?                                                | 4 | 2 | 0 | 0 |
| 16 | Apakah Anda mewajibkan mitra bisnis untuk menjaga kerahasiaan, seperti menyertakan klausul kerahasiaan (kewajiban untuk menjaga kerahasiaan) dalam kontrak?                                                                                                             | 4 | 2 | 0 | 0 |
| 17 | Apakah Anda menerapkan langkah untuk membatasi akses administratif karyawan terhadap data usaha (perusahaan) secara spesifik sesuai dengan deskripsi tugasnya?                                                                                                          | 4 | 2 | 0 | 0 |

|                                |                                                                                                                                                                                                        |                            |   |   |   |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|---|---|---|
| 18                             | Apakah Anda selalu memastikan bahwa <i>firewall</i> pada komputer dan/atau laptop selalu aktif dengan tujuan untuk melindungi aset penting Anda dari ancaman/serangan siber melalui jaringan internet? | 4                          | 2 | 0 | 0 |
| 19                             | Apakah Anda menerapkan penggunaan kata sandi ( <i>password</i> ) dan enkripsi (misal: WPA2-PSK) pada jaringan WiFi milik usaha (perusahaan) Anda?                                                      | 4                          | 2 | 0 | 0 |
| 20                             | Apakah Anda menginstal antivirus dan mengatur pembaruan antivirus secara otomatis?                                                                                                                     | 4                          | 2 | 0 | 0 |
| 21                             | Apakah Anda memastikan bahwa email yang Anda terima aman dari peretas yang ingin mendapatkan akses ke jaringan Anda ( <i>email phishing</i> )?                                                         | 4                          | 2 | 0 | 0 |
| 22                             | Apakah Anda sudah melakukan pemantauan aktivitas <i>log</i> (catatan digital) terhadap akun yang melakukan akses terhadap sistem Anda?                                                                 | 4                          | 2 | 0 | 0 |
| 23                             | Apakah Anda memiliki rencana tindak untuk menangani kebocoran, kehilangan, atau pencurian aset penting usaha (perusahaan)?                                                                             | 4                          | 2 | 0 | 0 |
| 24                             | Apakah Anda melakukan pencadangan rutin guna mencegah agar informasi penting tidak hilang karena kegagalan fungsi atau kesalahan operasi?                                                              | 4                          | 2 | 0 | 0 |
| 25                             | Apakah Anda mempelajari dan membagikan informasi tentang ancaman dan metode serangan siber terbaru terhadap aplikasi, komputer, laptop, dan/atau <i>smartphone</i> kepada internal usaha (perusahaan)? | 4                          | 2 | 0 | 0 |
| <b>HASIL PENILAIAN MANDIRI</b> |                                                                                                                                                                                                        | <b>Total DM + Total DS</b> |   |   |   |
|                                |                                                                                                                                                                                                        | .....                      |   |   |   |

★ Tidak ada jaminan bahwa langkah-langkah yang dijelaskan dalam lembar **PAMAN KAMI Versi 2.0** dapat menawarkan perlindungan lengkap.



## PENJELASAN KERENTANAN DAN LANGKAH PROTEKSI

| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | <p>Aset adalah semua kekayaan yang dipunyai oleh individu ataupun kelompok yang berwujud maupun tidak berwujud, yang memiliki nilai akan memiliki manfaat bagi setiap orang atau perusahaan.</p> <p>Aset merupakan bagian penting dalam sebuah usaha (perusahaan). Aset bukan hanya dalam bentuk uang tunai, tanah, bangunan, peralatan, ataupun perlengkapan yang lainnya. Namun aset juga dapat berupa informasi perusahaan yang di dalamnya juga meliputi sumber daya perusahaan, seperti SDM, informasi digital, pelanggan, dan sebagainya.</p> <p>Identifikasi adalah penentu atau penetapan identitas seseorang, benda, dan sebagainya (KBBI).</p> <p>Tujuan melakukan identifikasi aset penting perusahaan adalah agar keamanan aset penting lebih terjamin dan lebih mudah dalam menentukan langkah manajemen risiko terhadap asset tersebut.</p> <p>Kerentanan jika tidak dilakukan identifikasi aset penting:</p> | <ol style="list-style-type: none"> <li>Buatlah daftar seluruh aset yang Anda miliki saat ini baik yang berwujud maupun tidak berwujud.</li> <li>Buatlah kategori yang dapat memetakan aset penting yang harus dilindungi.</li> <li>Buatlah peringkat aset penting yang jika hilang akan berdampak pada bisnis Anda.</li> <li>Berikut dapat Anda pertimbangkan sebagai aset informasi penting perusahaan: <ul style="list-style-type: none"> <li>Alamat karyawan dan slip gaji.</li> <li>Daftar pembayaran untuk setiap mitra bisnis dan informasi transaksi.</li> <li>Informasi akuntansi organisasi Anda.</li> <li>Daftar kontak pelanggan dan mitra bisnis.</li> <li>Informasi pengembangan seperti gambar desain untuk produk baru.</li> <li>Setiap informasi dari mitra bisnis yang harus ditangani dengan hati-hati.</li> </ul> </li> </ol> |

| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>a. Tidak mengetahui aset penting yang dimilikinya</p> <p>b. lemahnya perlindungan terhadap aset tersebut.</p> <p>c. Rentan terhadap pencurian, penghapusan, penghilangan, perusakan.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 2  | <p>Manajemen risiko sangat penting untuk menyadarkan <i>top management</i> terhadap bahaya dan risiko dari aset yang dimiliki.</p> <p>Penerapan manajemen risiko sangat membantu perusahaan untuk mengelola ketidakpastian yang mungkin terjadi karena perusahaan bisa menyusun rencana pengendalian dan pencegahan sehingga kerugian perusahaan dapat dicegah atau dikurangi.</p> <p>Tujuan identifikasi risiko untuk menemukan atau mengetahui risiko-risiko yang mungkin timbul dalam kegiatan yang dilakukan oleh perusahaan atau perorangan.</p> <p>Kerentanan jika tidak dilakukan penilaian risiko terhadap aset penting adalah meningkatnya kerugian yang harus ditanggung oleh perusahaan apabila terjadi permasalahan terhadap aset yang dimiliki.</p> | <p>a. Identifikasi Risiko merupakan langkah awal dalam siklus Manajemen Risiko. Adapun proses identifikasi risiko adalah sebagai berikut:</p> <ul style="list-style-type: none"> <li>▪ Menentukan unit risiko</li> <li>▪ Memahami proses bisnis usaha (perusahaan)</li> <li>▪ Menentukan aktivitas krusial</li> <li>▪ Menentukan barang dan orang pada aktivitas krusial tersebut</li> <li>▪ Menentukan bentuk kerugian yang dapat terjadi pada barang dan orang dari aktivitas krusial tersebut</li> <li>▪ Menentukan penyebab terjadinya kerugian atau risiko.</li> </ul> <p>b. Salah satu acuan untuk melakukan identifikasi risiko dapat dilihat pada ISO 31000: 2018 <i>Risk Management–Principles and Guidelines</i>.</p> |

| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3  | <p>Meskipun pimpinan telah menetapkan kebijakan tentang langkah keamanan informasi, masih ada kemungkinan karyawan melakukan kelalaian atau pelanggaran. Kecuali jika kebijakan tersebut secara jelas didokumentasikan sebagai aturan internal. Karyawan harus selalu meminta saran dari manajer/pimpinan mereka.</p> <p>Agar karyawan dapat bertindak mandiri sesuai dengan aturan, pendokumentasian "aturan perusahaan" secara jelas sangatlah penting sehingga karyawan dapat merujuk pada kebijakan tersebut kapan saja.</p> <p>Kerentanan jika tidak adanya kebijakan keamanan informasi sebagai berikut:</p> <ol style="list-style-type: none"> <li>Karyawan tidak memiliki pengetahuan dan kompetensi dalam menyikapi aset penting Usaha (perusahaan).</li> <li>Karyawan mengabaikan pentingnya perlindungan terhadap aset penting.</li> <li>Risiko hilangnya aset penting sangat mungkin terjadi.</li> </ol> | <ol style="list-style-type: none"> <li>Menyusun kebijakan keamanan informasi yang berdasarkan hasil identifikasi aset, penilaian risiko, dan melibatkan <i>stakeholder</i>.</li> <li>Mensosialisasikan kebijakan keamanan informasi kepada seluruh <i>stakeholder</i> usaha (perusahaan).</li> <li>Memantau penerapan kebijakan keamanan informasi agar aset yang dilindungi dalam kondisi terjaga keamanannya.</li> <li>Meninjau dan mengevaluasi penerapan kebijakan keamanan informasi secara rutin guna memperbaikinya jika terdapat kekurangan.</li> <li>Melakukan revisi kebijakan keamanan informasi sesuai dengan hasil peninjauan dan evaluasi penerapan kebijakan keamanan informasi.</li> </ol> |
| 4  | <p>Kata Sandi atau <i>password</i> merupakan sekumpulan karakter yang digunakan oleh pengguna suatu perangkat, jaringan, sistem</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <ol style="list-style-type: none"> <li>Mengaktifkan fitur <i>user password</i> untuk mengakses perangkat seperti komputer, laptop, dan <i>smartphone</i>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | LANGKAH PROTEKSI                                                                                                            |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
|    | <p>operasi atau aplikasi yang mendukung banyak pengguna (<i>multiuser</i>) untuk memverifikasi identitas dirinya terhadap suatu perangkat, jaringan, sistem operasi atau aplikasi tersebut.</p> <p>Tujuan dari penggunaan <i>password</i> pada komputer, laptop, dan/atau <i>smartphone</i> adalah:</p> <ol style="list-style-type: none"> <li>Menjaga keamanan informasi dan akun.</li> <li>Menjadi batasan pelanggaran ke beberapa akun.</li> <li>Mencegah peretas mengakses aplikasi secara konstan.</li> <li>Mencegah penyalahgunaan informasi penting.</li> <li>Membatasi akses yang diperoleh <i>logger keystroke</i>.</li> </ol> <p>Kerentanan akan terjadi jika tidak ada kebijakan keamanan informasi pada perangkat komputer, laptop, dan/atau <i>smartphone</i> yang tidak menggunakan kata sandi (<i>password</i>) seperti, <i>pencurian</i> maupun penyalahgunaan informasi maupun data penting yang terdapat pada perangkat tersebut.</p> | <ol style="list-style-type: none"> <li>melakukan manajemen kata sandi (informasi detail dapat dibaca di poin 5).</li> </ol> |



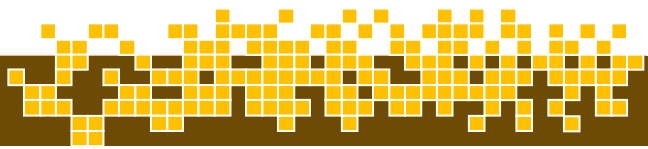
| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5  | <p>Kata Sandi atau <i>password</i> merupakan sekumpulan karakter yang digunakan oleh pengguna suatu perangkat, jaringan, sistem operasi atau aplikasi yang mendukung banyak pengguna (<i>multiuser</i>) untuk memverifikasi identitas dirinya terhadap suatu perangkat, jaringan, sistem operasi atau aplikasi tersebut.</p> <p>Tujuan dari menghindari penggunaan <i>password</i> yang sama untuk mengakses beberapa akun pada suatu sistem atau layanan web adalah untuk:</p> <ol style="list-style-type: none"> <li>Menjaga keamanan informasi dan akun.</li> <li>Menjadi Batasan pelanggaran ke beberapa akun.</li> <li>Mencegah peretas mengakses aplikasi secara konstan.</li> <li>Mencegah penyalahgunaan informasi penting.</li> <li>Membatasi akses yang diperoleh <i>logger keystroke</i>.</li> </ol> <p>Kerentanan yang ditimbulkan apabila menggunakan kata sandi atau <i>password</i> yang sama untuk mengakses beberapa layanan aplikasi web adalah peretas dapat mengakses aplikasi secara konstan dan</p> | <p>Sebelum bicara tentang manajemen kata sandi, kita harus memahami aturan penting dalam membuat kata sandi yang kuat, yaitu jangan pernah membuat kata sandi dengan suku kata umum.</p> <p>Membuat kata sandi dengan menggunakan campuran huruf, angka, tanda baca dan simbol tipografi seperti "<b>@Pr0t3d16%!</b>".</p> <p>Berikut beberapa tip untuk manajemen kata sandi:</p> <ol style="list-style-type: none"> <li>Jangan gunakan kata sandi yang sama pada semua layanan web, platform atau perangkat Anda.</li> <li>Selalu ganti (<i>refresh</i>) kata sandi pada perangkat/gawai komputer, <i>smartphone</i>, <i>router</i> Wi-Fi secara berkala/periodik (30, 60 atau 90 hari).</li> <li>Katakan TIDAK/NO apabila situs web meminta untuk "mengingat\remember" kata sandi Anda.</li> <li>Jangan menyimpan kata sandi di <i>hard disk/memory</i> tanpa dienkripsi alias <i>Plain Text</i>.</li> <li>Jangan menyimpan kata sandi sembarangan di tempat yang dapat diakses secara bebas oleh umum atau orang lain.</li> <li>Jangan berikan kata sandi Anda kepada siapa pun dikarenakan kata sandi merupakan</li> </ol> |



| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | memperbesar risiko terhadap pencurian maupun penyalahgunaan informasi maupun data penting yang terdapat pada perangkat tersebut apabila <i>password</i> tersebut sudah bocor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | kredensial terhadap identitas Anda untuk mengakses sistem.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 6  | <p>Dokumen yang berisikan informasi penting harus diberikan perlakuan yang khusus untuk menghindari hilang atau bocornya informasi penting tersebut dari pihak yang tidak berhak. Upaya perlakuan khusus terhadap informasi penting yang dapat dilakukan seperti menyimpannya pada kabinet/lemari/laci yang terkunci dan tidak meninggalkannya di atas meja tanpa adanya pengamanan khusus.</p> <p>Meninggalkan informasi/ dokumen tanpa pengawasan di atas meja merupakan tindakan berbahaya karena rentan terhadap pencurian atau sekedar diambil atau dibaca oleh seseorang. Apabila dokumen tersebut bersifat penting atau rahasia, maka dokumen tersebut dapat dicuri sehingga mengakibatkan kerugian pada usaha atau perusahaan.</p> | <ol style="list-style-type: none"> <li>Terapkan perlakuan khusus terhadap Informasi/dokumen penting untuk mencegah orang lain melihat, menyentuh, membaca, mengambil, dan/atau menyalinnya.</li> <li>Terapkan upaya untuk dapat memastikan bahwa informasi/ dokumen berada dalam pengawasan.</li> <li>Tentukan lokasi penyimpanan informasi/dokumen. Keluarkan informasi/dokumen hanya jika diperlukan untuk bekerja, dan pastikan untuk menyimpannya kembali setelah selesai.</li> <li>Menerapkan 5R (Ringkas, Rapi, Resik, Rawat, dan Rajin), serta menyimpan informasi/dokumen penting dalam kabinet yang terkunci.</li> </ol> |

| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                                                                |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7  | <p>Terdapat potensi bahaya pencurian informasi jika Anda tidak membatasi akses bagi orang yang tidak berwenang untuk memasuki area kerja terbatas milik usaha (perusahaan).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               | <p>Terapkan langkah pencegahan, seperti mendekati seseorang yang tidak Anda kenal di kantor, menyiapkan meja resepsionis maupun memberikan tanda pada area kerja terbatas milik usaha (perusahaan).</p> <p>Pastikan, kontrol, dan batasi orang yang tidak berhak dan tidak diizinkan untuk mengakses informasi/dokumen penting, terutama seperti <i>server</i>, arsip, dan brankas.</p>                                         |
| 8  | <p><i>Surge Protector</i> digunakan untuk melindungi jaringan Anda dari sambaran petir dan lonjakan listrik.</p> <p>UPS (<i>Uninterruptible Power Supply</i>) merupakan perangkat keras komputer yang berfungsi untuk memberikan suplai listrik ketika tegangan utama tidak berfungsi (terhenti, pemadaman listrik).</p> <p>Kerentanan yang ditimbulkan apabila perusahaan (usaha) tidak menggunakan perangkat tersebut adalah:</p> <p>a. <i>Surge Protector</i> melindungi seluruh jaringan dari kerusakan akibat lonjakan listrik yang dapat mengakibatkan hilangnya semua informasi penting Anda akibat dari kerusakan</p> | <p>a. Gunakan <i>Surge Protector</i> untuk menghubungkan perangkat <i>wireless</i> Anda dengan antena eksternal sehingga melindungi seluruh jaringan anda dari kerusakan akibat lonjakan listrik.</p> <p>b. Gunakan UPS pada setiap komputer anda. UPS memungkinkan Anda bekerja melalui pemadaman listrik dengan waktu tertentu namun UPS mampu menyediakan waktu yang cukup untuk menyimpan data Anda saat listrik padam.</p> |

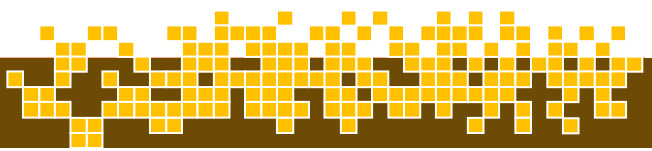
| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                 |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>perangkat penyimpanan informasi tersebut.</p> <p>b. UPS sangat cocok dipakai di perusahaan (usaha) Anda karena bisa menjaga dan melindungi komputer dari hal-hal yang yang tidak diinginkan, contoh nya jika listrik padam UPS akan melindungi dari hilangnya data yang belum di simpan atau pun dari kerusakan perangkat kerasnya sendiri.</p>                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                  |
| 9  | <p>Saat membuang atau menghapus informasi penting, Anda harus memastikan bahwa informasi tersebut sudah dihapus dengan menerapkan prosedur yang benar sehingga informasi tersebut menjadi tidak terbaca dan tidak bisa dipulihkan kembali.</p> <p>Kerentanan yang ditimbulkan apabila membuang dokumen berisi informasi penting ke tempat sampah tanpa memastikan bahwa informasi tersebut dihapus dengan benar atau menjadikannya tidak terbaca lagi adalah dapat menyebabkan kebocoran informasi serius karena orang lain akan dapat membaca dokumen tersebut. Selain itu, informasi yang disimpan pada perangkat elektronik dan media elektronik</p> | <p>a. Ambil langkah untuk memusnahkan informasi, seperti dengan menggunakan perangkat lunak penghapus data, atau meminta seorang spesialis untuk menghapusnya.</p> <p>b. Saat memusnahkan informasi penting bersifat fisik, musnahkan setiap bentuk informasi dengan tepat, seperti dengan menggunakan mesin penghancur kertas atau perangkat keras lainnya.</p> |



| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | juga dapat dipulihkan, meskipun file sudah dihapus.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 10 | <p>Wi-Fi publik atau yang juga disebut dengan “<i>hotspot</i>” umum merupakan hak akses internet menggunakan teknologi Wi-Fi melalui jaringan area lokal nirkabel (WLAN) dimana lokasi fisik tempat Anda berada. Wi-Fi publik biasanya dimanfaatkan oleh siapa saja yang tidak ingin memboroskan data seluler mereka. Alih-alih ingin menghemat, namun justru risiko mengancam aset penting yang Anda miliki.</p> <p>Kerentanan yang ditimbulkan saat Anda menggunakan jaringan internet Wi-Fi publik (misalnya di hotel atau kedai kopi) adalah Wi-Fi publik sebenarnya adalah titik paling mudah bagi orang lain untuk melihat informasi Anda. Ketika Anda menyambungkan perangkat Anda dengan jaringan Wi-Fi, Anda mengirimkan informasi pribadi Anda sendiri melalui situs web atau aplikasi ponsel, dan itu sangat mudah bagi para peretas untuk mencegat dan merusak informasi Anda.</p> <p>Selain itu tidak mudah untuk mencari tahu siapa pemilik dan</p> | <p>a. Tindakan pencegahan paling sederhana adalah tidak menghubungkan komputer, laptop, dan <i>smartphone</i> ke jaringan Internet yang menggunakan Wi-Fi publik, namun disarankan untuk menggunakan ‘<i>tethering</i>’ (di mana perangkat Anda yang lain seperti <i>smartphone</i> berbagi koneksi 3G / 4G Anda), atau ‘<i>dongle</i>’ nirkabel yang disediakan oleh jaringan seluler Anda.</p> <p>b. Jika terhubung dengan Wi-Fi publik, Anda harus memastikan apabila jaringan tersebut legal, hindari melakukan transaksi perbankan atau perdagangan untuk menghindari hal-hal yang tidak diinginkan.</p> <p>c. Anda juga dapat menggunakan Jaringan Pribadi Virtual (VPN).</p> <p>d. Aktifkan <i>Firewall</i> pada perangkat yang Anda gunakan.</p> <p>e. Matikan fitur berbagi file (<i>file sharing</i>) pada perangkat Anda melalui menu pengaturan jaringan. Usahakan juga untuk meminimalkan jumlah data pribadi yang disimpan pada perangkat tersebut.</p> |

| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>yang mengendalikan Wi-Fi publik tersebut. Jika Anda terhubung ke <i>hotspot</i> ini, orang lain dapat:</p> <ol style="list-style-type: none"> <li>Memonitor apa yang sedang Anda kerjakan di dunia maya.</li> <li>Mengetahui detail akun pribadi yang Anda kelola saat Anda melakukan <i>login</i> maupun melakukan transaksi.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 11 | <p>Serangan rekayasa sosial (<i>social engineering</i>) merupakan upaya manipulasi psikologis seseorang dengan tujuan untuk mendapatkan informasi/hak akses tertentu dengan cara menipu korbannya secara halus tanpa korban tersebut meyadarinya. Serangan ini dapat dilakukan dengan cara:</p> <ol style="list-style-type: none"> <li>Menggunakan suara<br/>Saat menipu seseorang, penipu bisa berbicara untuk meyakinkan korban.</li> <li>Menggunakan gambar/video<br/><i>Spammer</i> memasang gambar/video yang erotis/menarik agar di klik oleh korban.</li> <li>Menggunakan tulisan<br/>Peretas menulis artikel yang persuasif dan meyakinkan misalnya, dengan menulis tutorial cara membobol akun facebook, tetapi akhirnya</li> </ol> | <ol style="list-style-type: none"> <li>Batasi Informasi publik<br/>Batasi informasi pribadi yang Anda bagikan secara <i>online</i>.</li> <li>Bersikap skeptis<br/>Selalu mempertanyakan permintaan informasi yang sensitif.</li> <li>Verifikasi<br/>Jangan berbagi informasi sebelum Anda dapat memverifikasi segala bentuk permintaan melalui media apapun.</li> <li><i>No Password</i><br/>Jangan pernah membagikan kata sandi Anda kepada siapa pun.</li> </ol> |

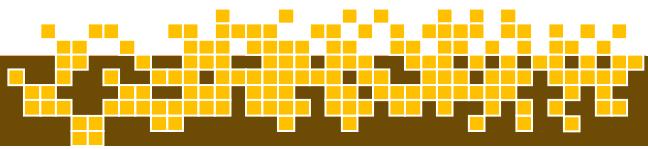
| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | LANGKAH PROTEKSI                                                                                                                                                                                                                                                          |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>korban dituntun untuk menginstall <i>tools hacking</i> yang aslinya adalah <i>malware</i>.</p> <p>Kerentanan yang ditimbulkan dari serangan <i>social engineering</i> (rekayasa sosial) adalah bocornya informasi penting milik pribadi atau perusahaan (usaha) secara langsung melalui target tanpa target tersebut menyadarinya.</p>                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                           |
| 12 | <p>Setiap <i>Operating System, smartphone</i>, perangkat lunak dan aplikasi selalu menyediakan pembaharuan (<i>update</i>) secara periodik maupun insidental terhadap perangkat mereka dengan tujuan untuk meningkatkan keamanan dan peforma, dukungan teknologi baru, kompatibilitas, dan mengatasi permasalahan atau <i>bug</i> pada versi sebelumnya.</p> <p>Kerentanan yang ditimbulkan akibat dari mengabaikan pembaharuan (<i>update</i>) pada <i>Operating System, smartphone</i>, dan perangkat lunak lainnya adalah membuat perangkat Anda rentan terinfeksi virus berbahaya yang belum bisa terdeteksi pada versi sebelumnya.</p> | <ol style="list-style-type: none"> <li>Memastikan perangkat terhubung ke jaringan internet yang aman.</li> <li>Fitur pembaruan diaktifkan secara otomatis.</li> <li>Terapkan <i>patch</i> pembaharuan (<i>update</i>) ke perangkat atau gunakan versi terbaru.</li> </ol> |



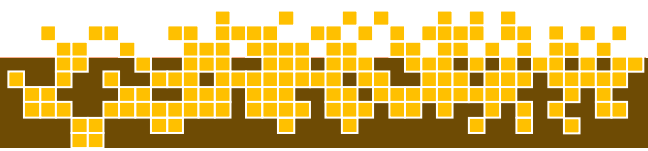
| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 13 | <p>Aplikasi yang berasal dari sumber tidak tepercaya, dengan kata lain aplikasi yang diunduh berasal dari sumber yang tidak resmi/aplikasi bajakan. Tentunya aplikasi yang seperti ini menimbulkan banyak kerugian bagi yang menginstalnya.</p> <p>Kerentanan keamanan informasi yang ditimbulkan akibat dari mengabaikan pentingnya memastikan bahwa aplikasi yang diunduh dan diinstal pada komputer, laptop, dan <i>smartphone</i> aman dan berasal dari sumber terpercaya yaitu perangkat Anda dapat terinfeksi atau tersusupi oleh <i>malware</i> yang berbahaya.</p> | <ol style="list-style-type: none"> <li>Memastikan aplikasi yang diinstal pada perangkat berasal dari sumber terpercaya misalnya <i>Google Play</i> atau <i>Apple App Store</i> untuk <i>smartphone</i>.</li> <li>Mengaktifkan fitur <i>real time protection</i> pada Antivirus Anda.</li> <li>Mengaktifkan fitur notifikasi <i>pertanyaan keamanan unknown sources</i> pada <i>smartphone</i>.</li> </ol>                                                                                                                                                                    |
| 14 | <p>Internet yang disediakan perusahaan (usaha) merupakan fasilitas untuk memberi kemudahan, kenyamanan, kecepatan dan nilai tambah bagi pegawai dalam pencapaian target kinerja dan keuntungan organisasi. Pegawai dalam rangka pencapaian kinerja dapat menggunakan internet perusahaan untuk mengakses berbagai situs, mengunduh, menyimpan atau mengintalasi aplikasi tertentu. Oleh sebab, untuk mencegah dan mengendalikan Risiko dibutuhkan Kebijakan akses,</p>                                                                                                     | <ol style="list-style-type: none"> <li>Terapkan langkah, seperti membuat aturan akses untuk menggunakan Internet dan media sosial, dan gunakan filter web untuk secara sistematis membatasi penggunaan Internet ditempat kerja.</li> <li>Salah satu aturan yang dapat diberlakukan untuk mengontrol penggunaan Internet, seperti menetapkan aturan tentang menjelajahi situs web adalah menerapkan <i>web content filtering</i>. <i>Web content filtering</i> dapat digunakan oleh perusahaan (usaha) untuk melakukan penyaringan terhadap situs-situs yang tidak</li> </ol> |

| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>mengunduh, mengintalasi kode sumber tertentu.</p> <p>Kerentanan yang ditimbulkan apabila tidak adanya kebijakan atau aturan menjelajahi situs web dapat menyebabkan perangkat Anda terinfeksi malware atau virus.</p>                                                                                                                                                                                                                                                                                           | <p>diperbolehkan oleh perusahaan (usaha) maupun yang tidak berhubungan dengan tujuan bisnis agar tidak dapat diakses.</p> <p>c. Kendali konten melalui web <i>content filtering</i> nantinya akan menentukan konten apa saja yang tersedia maupun konten-konten yang tidak boleh diakses atau diblokir. Pembatasan tersebut dapat diterapkan di berbagai tingkatan: perorangan, kelompok, sekolah (pendidikan), organisasi, maupun pada penyedia jasa layanan internet (<i>Internet Service Provider</i>).</p> |
| 15 | <p>Salah satu ciri organisasi usaha yang tahan terhadap serangan siber adalah memahami bahwa keamanan informasi yang baik adalah tanggung jawab semua orang, bukan hanya unit/departemen TI. Peretas selalu menemukan cara baru untuk mengakses informasi, sehingga sangat penting untuk menciptakan budaya di mana karyawan menyadari dan memahami dampak dari serangan siber.</p> <p>Kerentanan jika tidak adanya program untuk memberikan pemahaman keamanan informasi bagi pegawai adalah sebagai berikut:</p> | <p>Terapkan langkah:</p> <p>a. memberikan pemahaman kepada pegawai secara rutin tentang budaya kesadaran keamanan informasi di lingkungan perusahaan merupakan tanggungjawab semua orang.</p> <p>b. Terapkan dalam merekrut pegawai dengan terlebih dahulu memeriksa profilnya.</p> <p>c. Terapkan penelitian personel yang ingin menjadi pegawai untuk mengetahui profil dan latar belakang calon pegawai.</p>                                                                                                |

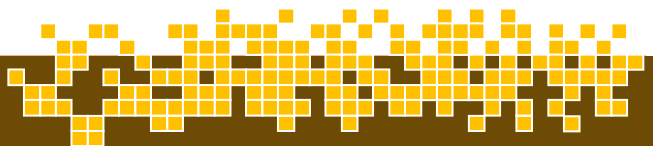
| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                   |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>a. Pegawai tidak memiliki pengetahuan dan kompetensi dalam keamanan informasi.</p> <p>b. Karyawan mengabaikan pentingnya keamanan informasi merupakan tanggung jawab semua orang yang bekerja pada usaha (perusahaan).</p> <p>c. Meningkatnya risiko hilangnya aset/informasi penting sangat mungkin terjadi.</p>                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                    |
| 16 | <p>Klausul kerahasiaan (kewajiban untuk menjaga kerahasiaan) merupakan klausul yang sangat disarankan untuk ditambahkan pada perjanjian kerjasama dengan mitra bisnis. Hal ini penting sebagai langkah perlindungan terhadap aset atau informasi penting milik perusahaan Anda yang secara langsung maupun tidak langsung dibagikan kepada mitra bisnis Anda.</p> <p>Kerentanan yang ditimbulkan dengan tidak adanya klausul kerahasiaan secara spesifik dalam kontrak perjanjian kerjasama adalah:</p> <p>a. Mitra bisnis dapat memanfaatkan dan menyalahgunakan informasi rahasia milik perusahaan.</p> | <p>a. Ambil langkah, seperti mencantumkan klausul kerahasiaan pada perjanjian kerjasama dengan mitra bisnis.</p> <p>b. Ketika memberikan informasi rahasia kepada mitra bisnis, perlu dijelaskan bahwa informasi tersebut harus diperlakukan sebagaimana perlakuan terhadap informasi rahasia.</p> |



| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                                 |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>b. Mitra bisnis dapat menjual informasi rahasia perusahaan kepada pihak yang membutuhkan.</p> <p>c. Mitra bisnis memanfaatkannya untuk kepentingan bisnisnya sendiri.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                  |
| 17 | <p>Pembatasan akses administratif dalam hal ini adalah seperti pembagian hak akses karyawan dalam suatu grup untuk mengakses data perusahaan sesuai dengan deskripsi tugasnya. Ini dilakukan untuk melindungi data perusahaan dari karyawan yang tidak memiliki kepentingan terhadap data tersebut sehingga akibat buruk yang ditimbulkan dari penyalahgunaan atau pencurian informasi tersebut dapat dihindari atau diminimalisasi.</p> <p>Kerentanan yang ditimbulkan jika tidak adanya pembatasan akses administratif karyawan terhadap data perusahaan (usaha) sesuai deskripsi tugasnya, antara lain adalah adanya kemungkinan peretas (penyusup) dari luar atau dalam (karyawan) dapat mengakses lokasi yang sensitif atau sumber daya penting (rahasia) milik perusahaan, sehingga dapat dimanfaatkan</p> | <p>a. Pastikan Anda membatasi akses karyawan ke lokasi sensitif dan sumber daya.</p> <p>b. Terapkan kebijakan untuk membatasi akses administratif karyawan terhadap data kantor secara spesifik sesuai dengan deskripsi tugasnya untuk mencegah seorang peretas mendapatkan akses ke jaringan kantor Anda. Misalnya, hanya memungkinkan staf TI yang berwenang untuk mengakses ruang server.</p> |

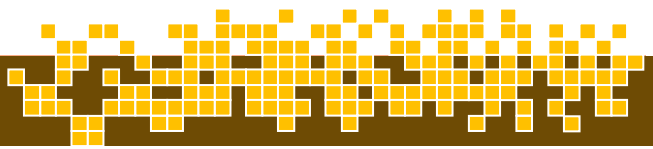


| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | untuk tujuan yang dapat merugikan perusahaan (usaha).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 18 | <p><i>Firewall</i> merupakan perangkat sistem keamanan untuk mengelola dan memantau trafik masuk dan keluar berdasarkan aturan keamanan (<i>security rules</i>) yang sudah ditentukan. <i>Firewall</i> berfungsi mencegah akses yang tidak diinginkan dari atau ke dalam jaringan, komputer, laptop dan/atau server.</p> <p><i>Firewall</i> memiliki beberapa fungsi diantaranya adalah sebagai berikut:</p> <ol style="list-style-type: none"> <li>Melindungi data dari peretas dan pengguna yang tidak terotorisasi.</li> <li>Mencegah pesan yang tidak diinginkan.</li> <li>Mencegah konten yang tidak diinginkan.</li> <li>Monitoring <i>bandwidth</i>.</li> </ol> <p>Kerentanan yang ditimbulkan dengan tidak diaktifkannya <i>Firewall</i> pada komputer atau laptop Anda adalah peretas dan/atau pengguna yang tidak memiliki otorisasi dapat masuk kedalam jaringan dan mencuri data komputer atau laptop Anda.</p> | <ol style="list-style-type: none"> <li>Atur konfigurasi, terapkan, dan pastikan <i>firewall</i> pada komputer atau laptop selalu aktif.</li> <li><i>Firewall</i> adalah sistem keamanan yang melindungi komputer atau laptop Anda dari berbagai ancaman di jaringan internet. <i>Firewall</i> ini bekerja sebagai sekat atau tembok yang membatasi komputer dari jaringan internet. Salah satu fungsi <i>Firewall</i> adalah melindungi data dari peretas dan pengguna tidak terotorisasi yang akan mencuri data komputer atau laptop Anda.</li> </ol> |
| 19 | <p>Wi-Fi (<i>Wireless Fidelity</i>) merupakan salah satu media</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <ol style="list-style-type: none"> <li>Pastikan untuk mengatur keamanan jaringan <i>wireless</i> di</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                         |



| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                              |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>transmisi data tanpa menggunakan kabel. Wi-Fi rentan dari serangan karena siapa saja bisa masuk kedalam jaringan. Untuk mengatasinya, maka diperlukanlah enkripsi. Dengan adanya enkripsi, maka Wi-Fi Anda akan lebih aman. Jaringan <i>wireless</i> milik perusahaan (usaha) harus di enkripsi dan memiliki <i>password</i> yang kuat untuk mengakses jaringan tersebut.</p> <p>Kerentanan yang ditimbulkan dari jaringan <i>wireless</i> yang tidak memiliki pengaturan keamanan yang memadai berpotensi mengalami kebocoran atau penyalahgunaan data untuk tindakan kriminal dengan menghubungkannya secara ilegal ke pencuri data.</p> | <p>perusahaan Anda untuk mencegah penyadapan dan penggunaan yang tidak sah.</p> <p>b. Ambil langkah, seperti menggunakan pengaturan enkripsi (mis. WPA2-PSK) dan menggunakan frase sandi yang panjang dan sulit ditebak. (Petunjuk pembuatan kata sandi atau <i>password</i> yang baik dapat dilihat pada poin nomor 5).</p>  |
| 20 | <p>Antivirus adalah sebuah perangkat lunak (<i>software</i>) komputer yang berfungsi untuk melindungi komputer dari serangan virus. Antivirus ini akan memberikan perlindungan dan keamanan pada data dan sistem yang ada pada komputer Anda sehingga pengguna komputer tersebut akan merasa aman dan nyaman dalam menyimpan data mereka.</p>                                                                                                                                                                                                                                                                                                 | <p>a. Instal perangkat lunak antivirus.</p> <p>b. Atur perangkat agar secara otomatis memperbarui file definisi virus.</p> <p>c. Pertimbangkan untuk menginstal perangkat lunak keamanan terkonsolidasi.</p> <p>d. Ambil langkah untuk menghadapi metode ancaman dan serangan dengan cara mempelajarinya terlebih dahulu.</p> |

| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                         |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>Beberapa kerentanan yang ditimbulkan apabila tidak menginstal antivirus dan mengatur pembaruan antivirus secara otomatis adalah terjadi peningkatan jumlah serangan <i>phishing</i> untuk mencuri <i>User ID</i>, <i>password</i> dan data-data penting lainnya melalui <i>email</i> dengan virus yang menyamar sebagai mitra bisnis, pemangku kepentingan lainnya, dan/atau mengarahkan seseorang untuk membuka situs web palsu yang meniru situs web yang sah.</p>                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                          |
| 21 | <p><i>Email Phishing</i> adalah tindakan memperoleh informasi pribadi seperti <i>User ID</i>, <i>password</i> dan data-data penting lainnya dengan menyamar sebagai orang atau organisasi yang berwenang melalui sebuah email.</p> <p>Kerentanan yang ditimbulkan dari <i>Email Phishing</i> adalah dapat mengelabui pengguna agar memberikan kredensial akses <i>login</i> atau memulai transaksi penipuan, serta tanpa sadar menginstal <i>malware</i>, <i>ransomware</i>, dan muatan berbahaya lainnya. Disinilah peretas menemukan celah untuk melakukan serangan siber berbasis email (<i>Email Phishing</i>).</p> | <ol style="list-style-type: none"> <li>Lakukan filter spam.</li> <li>Waspada terhadap email yang tidak dikenali pengirimnya.</li> <li>Hati-hati terhadap lampiran email, jangan pernah membuka lampiran apabila dirasa mencurigakan.</li> <li>Pasang software antivirus yang selalu <i>Up to Date</i>.</li> <li>Aktifkan <i>Firewall</i> pribadi dan tetap <i>up to date</i>.</li> </ol> |



| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 22 | <p>Monitoring aktivitas atau <i>log</i> digunakan untuk mengetahui aktifitas yang tidak biasa pada sistem Anda sebagai langkah untuk mengambil keputusan terhadap perlindungan sistem Anda</p> <p>Perangkat keras atau perangkat lunak misalnya Firewall atau Antivirus seringkali memiliki kemampuan untuk menyimpan catatan <i>log</i> atau aktivitas. <i>Log</i> dapat digunakan untuk mengidentifikasi aktivitas mencurigakan dan sangat berharga apabila digunakan untuk proses investigasi terhadap adanya insiden siber. <i>Log File</i> berisi catatan otomatis dari semua atau beberapa kegiatan pada sistem komputer.</p> <p>Kerentanan yang ditimbulkan apabila tidak melakukan monitoring aktivitas <i>log</i> serta menyimpan file catatan <i>log</i> tersebut adalah sebagai berikut:</p> <ol style="list-style-type: none"> <li>Anda atau usaha (perusahaan) Anda tidak dapat mengetahui aktifitas yang tidak biasa pada sistem anda sebagai langkah untuk mengambil keputusan terhadap perlindungan sistem Anda.</li> <li>Terdapat kendala pada proses investigasi apabila</li> </ol> | <ol style="list-style-type: none"> <li>Pastikan fungsionalitas <i>log</i> pada perangkat keras atau perangkat lunak Anda aktif.</li> <li>Simpan <i>log</i> setidaknya dalam kurun waktu satu tahun. Beberapa informasi <i>log</i> mungkin perlu disimpan dalam kurun waktu enam tahun.</li> <li>Anda dapat melakukan monitoring terhadap <i>log</i> untuk mengetahui aktifitas yang tidak biasa pada sistem Anda sebagai langkah untuk mengambil keputusan terhadap perlindungan sistem Anda.</li> </ol> |



| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                         |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | usaha (perusahaan) Anda terkena serangan siber.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                          |
| 23 | <p>Ketika suatu insiden terjadi, biasanya tidak ada waktu untuk berpikir dengan tenang, dan keterlambatan dalam menanggapi insiden tersebut cenderung akan memperparah dampak dari insiden tersebut.</p> <p>Kerentanan yang ditimbulkan apabila usaha (perusahaan) tidak memiliki pedoman rencana tindak untuk menangani kebocoran, kehilangan, atau pencurian aset penting usaha (perusahaan) adalah sebagai berikut:</p> <ol style="list-style-type: none"> <li>Terhambatnya langkah penanganan insiden siber sehingga dapat memperparah dampak yang ditimbulkannya.</li> <li>Waktu yang dibutuhkan untuk pemulihan terkait insiden tersebut semakin lama sehingga semakin memperbesar kerugian yang ditimbulkan.</li> </ol> | <ol style="list-style-type: none"> <li>Ambil langkah, seperti menyiapkan pedoman rencana tindak untuk informasi penting yang bocor, hilang, atau dicuri.</li> <li>Gunakan referensi terhadap insiden yang pernah dilaporkan di media untuk memikirkan siapa dan kapan akan melakukan apa, dengan asumsi bahwa hal yang sama dapat terjadi di perusahaan Anda.</li> </ol> |
| 24 | <p>Backup data adalah proses membuat data cadangan dengan cara menyalin atau membuat arsip data komputer sehingga data tersebut dapat digunakan kembali apabila</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <ol style="list-style-type: none"> <li>Identifikasi data penting yang Anda butuhkan untuk dicadangkan.</li> <li>Menyimpan cadangan di lokasi terpisah dan tidak terkoneksi dengan internet secara terus menerus misalnya dengan</li> </ol>                                                                                                                               |

| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | LANGKAH PROTEKSI                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>terjadi kerusakan atau kehilangan.</p> <p>Tujuan <i>Backup</i> data adalah sebagai berikut:</p> <ol style="list-style-type: none"> <li>Mengembalikan data apabila data tersebut hilang, baik karena terhapus atau karena rusak (<i>corrupt</i>).</li> <li>Mengembalikan data ke titik tertentu pada masa lalu.</li> </ol> <p>Kerentanan yang ditimbulkan apabila Anda atau usaha (perusahaan) Anda tidak melakukan pencadangan rutin adalah tidak bisa dipulihkannya data yang hilang akibat kegagalan fungsi, kesalahan operasi, atau infeksi virus.</p> | <p>menggunakan <i>portable hard drives</i> atau <i>cloud storage</i>.</p> <ol style="list-style-type: none"> <li>Apabila Anda menggunakan <i>cloud storage</i> untuk menyimpan cadangan data, baca panduan keamanan <i>cloud storage</i>.</li> <li>Lakukan pencadangan data penting secara rutin.</li> </ol>                                                                                                                                                                                   |
| 25 | <p>Salah satu ciri organisasi usaha yang tahan terhadap serangan siber adalah selalu mempelajari dan membagikan informasi tentang ancaman dan metode serangan siber terbaru terhadap aplikasi, komputer, laptop, dan/atau <i>smartphone</i> kepada internal usaha (perusahaan). Peretas selalu menemukan cara baru untuk mengakses informasi, sehingga sangat penting untuk menciptakan budaya dimana karyawan menyadari dan memahami dampak dari serangan siber.</p>                                                                                        | <p>Ambil langkah, seperti memeriksa situs web tentang keamanan siber dan berlangganan majalah untuk mempelajari metode ancaman dan serangan terbaru, mengonfirmasi peringatan yang diberikan oleh layanan <i>internet banking</i> dan layanan lain yang digunakan, serta membagikan informasi tentang serangan siber tersebut kepada internal perusahaan. Sehingga seluruh pegawai dapat melakukan tindakan preventif bahkan mempunyai solusi penanganan apabila insiden tersebut terjadi.</p> |

| NO | PENJELASAN KERENTANAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | LANGKAH PROTEKSI |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
|    | <p>Kerentanan jika tidak adanya program untuk memberikan pemahaman keamanan informasi bagi pegawai adalah sebagai berikut:</p> <ol style="list-style-type: none"> <li>Pegawai tidak memiliki pengetahuan dan kompetensi dalam keamanan informasi.</li> <li>Karyawan maupun internal usaha (perusahaan) tidak memiliki Informasi terkini tentang ancaman dan metode serangan siber terbaru terhadap aplikasi, komputer, laptop, dan/atau <i>smartphone</i>.</li> <li>Meningkatnya risiko hilangnya aset/informasi penting sangat mungkin terjadi akibat informasi serangan siber dan langkah pemulihannya yang sudah kedaluarsa.</li> </ol> |                  |

### Referensi:

1. Australian Government, 2017. *Cyber Security: The Small Business Best Practice Guide*. Australia: Australian Small Business and Family Enterprise Ombudsman.
2. Asean Japan Cyber Security Cooperation, 2019. *5 Menit Penilaian Mandiri Perusahaan terkait Keamanan Informasi*.
3. BSSN, 2019. *Tips Singkat dan Praktis di Dunia Siber, Dari BSSN untuk Masyarakat*. Jakarta: BSSN
4. NIST, 2016. *Small Business Information Security: The Fundamentals*. USA: U.S. Department of Commerce.
5. National Cyber Security Centre. *Cyber Security: Small Business Guide*.
6. OPTUS. *A Small business Guide to Effective Cyber Security*.



7. University of Southern Maine. Small Business Cyber Security Guide.



## RIWAYAT PERUBAHAN PRA LAUNCHING

Sehubungan dengan adanya perkembangan dan dinamika, **PAMAN KAMI Versi 1.1** merupakan perubahan dari **Versi 1.0**. Perubahan tersebut dilakukan oleh Baderi dan Eko Tulus Budi Cahyanto pada tanggal **20 September 2019** di Jakarta berdasarkan hasil ujicoba dan validasi instrumen PAMAN KAMI pada pelaku usaha bersama Auditor Keamanan Informasi di Kota Balikpapan. Adapun isi perubahannya adalah sebagai berikut: **Pertama**, penyesuaian substansi pada pertanyaan nomor 4, 6, 20, 21, 23, 24, dan 25. **Kedua**, rumusan, interval dan kelas interval setelah mengakomodasi *Statement of Applicability (SoA)*. **Ketiga**, PAMAN KAMI diupayakan menjadi lebih *user friendly*, salah satunya dengan merancang agar pelaku usaha atau *start-up* dapat mengisi instrumennya langsung dari gawainya masing-masing.

Tanggal **26 September 2019**, Baderi dan Eko Tulus Budi Cahyanto memperbarui PAMAN KAMI versi 1.1. menjadi **PAMAN KAMI Versi 1.2**. di Jakarta berdasarkan hasil ujicoba dan validasi instrumen PAMAN KAMI pada pelaku usaha di Kota Semarang. Adapun isi perubahannya adalah sebagai berikut: **Pertama**, PAMAN KAMI memiliki segmen berdasarkan pemetaan tingkatan pelaku usaha dari mikro hingga *hectacorn*. **Kedua**, penambahan isian identitas yang dibutuhkan oleh instrumen PAMAN KAMI seperti jenis kelamin, usia, pendidikan, nilai investasi, nilai aset, nilai omzet per tahun, dan jumlah tenaga kerja yang digunakan untuk usaha. **Ketiga**, penambahan pertanyaan yang relevan dengan kondisi dan kebutuhan Usaha Kecil dan Menengah.

Tanggal **05 Oktober 2019**, Baderi dan Eko Tulus Budi Cahyanto memperbarui PAMAN KAMI versi 1.2. menjadi **PAMAN KAMI Versi 1.3**. di Jakarta berdasarkan Hasil ujicoba dan validasi instrumen PAMAN KAMI pada para *start-up* di Kota Makassar. Di Kota Makassar, responden memberikan respon positif dan menyatakan bahwa keberadaan instrumen PAMAN KAMI sangat membantu.

Adapun isi perubahannya adalah sebagai berikut: **Pertama**, para pelaku *start-up* memberi masukan bahwa mereka kurang setuju jika disebut sebagai UKM dan lebih tepat disebut sebagai *startup*. Salah satu usulan mereka yaitu menambah isian identitas pada instrumen PAMAN KAMI seperti nama website, nama akun Instagram, nama akun Facebook, nama *merchant* di *marketplace* yang digunakan untuk usaha.

**Kedua**, identitas pemilik usaha, identitas usaha, dan media digital yang digunakan sangat dibutuhkan karena akan berpengaruh pada pelaku usaha

dalam menjawab pertanyaan-pertanyaan dalam PAMAN KAMI. **Ketiga**, perubahan judul menjadi PAMAN KAMI untuk UKM dan *Start-up*.

Tanggal **18 Oktober 2019**, Baderi dan Eko Tulus Budi Cahyanto melakukan perubahan secara signifikan pada PAMAN KAMI, sehingga PAMAN KAMI Versi 1.3. diubah menjadi **PAMAN KAMI Versi 2.0**. di Jakarta berdasarkan hasil uji coba dan validasi instrumen PAMAN KAMI pada para *start-up* di Kota Batam. Responden di Kota Batam memberikan respon yang baik dan menyatakan bahwa keberadaan instrumen PAMAN KAMI sangat membantu para pelaku usaha rintisan. Para pelaku usaha menilai susunan kalimat maupun istilah-istilah yang digunakan mudah dipahami karena mereka terbiasa bekerja dengan perangkat keras/lunak TIK. Dengan demikian, dapat disimpulkan bahwa instrumen PAMAN KAMI sudah valid, namun perlu adanya perubahan susunan item penilaian sesuai dengan siklus *Cybersecurity Framework*.

Adapun isi perubahannya adalah sebagai berikut: **Pertama**, perubahan susunan pertanyaan PAMAN KAMI Versi 1.3 yang sudah valid tersebut untuk disesuaikan siklusnya dengan menggunakan *Cybersecurity Framework* pada NISTIR 7621 Revisi 1 tentang *Small Business Information Security: The Fundamentals* sebagai pedoman dalam penyusunan item pertanyaan penilaian. Susunan pertanyaan penilaian dikelompokkan dalam kelompok identifikasi, proteksi, deteksi, penanggulangan, dan pemulihan, sehingga mudah dipahami siklusnya oleh *stakeholder*.

Perubahan item pertanyaan penilaian adalah sebagai berikut: **Perubahan Urutan V.1.3 ke V.2.0**. Nomor: 1 → 5, 2 → 4, 3 → 12, 4 → 20, 5 → 13, 6 → 11, 7 → 10, 8 → 21, 10 → 24, 11 → 6, 13 → 9, , 14 → 7, 15 → 14, 16 → 15, 18 → 17, 20 → 19, 21 → 25, 22 → 16, 24 → 23, dan 25 → 3. **Dihapus pada PAMAN KAMI Versi 1.3** Nomor: 9, 12, 17, 19, dan 23. **Item Pertanyaan Baru pada PAMAN KAMI Versi 2.0** Nomor: 1, 2, 8, 18, dan 22.

**Kedua**, melengkapi *form* identitas usaha (perusahaan), media digital usaha dan identitas pemilik usaha atau pengisi PAMAN KAMI. **Ketiga**, mengembalikan judul pedoman menjadi PAMAN KAMI untuk Usaha Kecil Menengah.





# PAMAN KAMI

*Penilaian Mandiri Keamanan Informasi*

ISBN 978-623-93005-0-0



Badan Siber dan Sandi Negara