Untuk UKM dan operator bisnis kecil

5 Menit Penilaian Mandiri Perusahaan terkait Keamanan Informasi

Apakah Anda sudah mendapat info tentang tren terbaru?

Perubahan ancaman dan serangan

- Ransomware
- Serangan daftar kata sandi
- Serangan email yang ditargetkan

Perubahan dalam lingkungan TI

- *Cloud*
- Tablet
- Ponsel pintar

Gunakan **"5 Menit Penilaian Mandiri Perusahaan terkait Keamanan Informasi"** untuk memeriksa status keamanan perusahaan Anda sebelum data Anda hilang!

ASEAN · JAPAN
Cybersecurity Cooperation

Penilaian Mandiri

1 Bacalah uraian berikut ini sebelum melakukan penilaian.

Cara penggunaan

Kami berfokus pada 25 langkah keamanan informasi yang efektif dan yang dapat diimplementasikan dengan biaya minim untuk organisasi. Periksalah status implementasi item-item ini, kemudian implementasikan langkah yang belum diambil sembari merujuk pada penjelasan dalam pamflet ini.

Cara membaca deskripsi

Buatlah penilaian tanpa mengandalkan contoh spesifik dalam deskripsi. Misalnya, inti dari pertanyaan no. 16 adalah tentang “langkah pencegahan pencurian.” Pertanyaan bertujuan untuk memastikan apakah Anda mengambil langkah untuk mencegah pencurian dengan meletakkan laptop di laci, jika organisasi Anda menggunakan laptop. Pertanyaan ini juga bertujuan untuk memastikan apakah Anda mengambil langkah untuk mencegah pencurian dengan tidak meninggalkan aksesori seperti stik USB atau ***hard drive*** eksternal di atas meja, jika organisasi Anda tidak memiliki laptop. Lihat pamflet jika Anda tidak mengerti tujuan dari suatu pertanyaan atau merasa sulit memahami pertanyaan tersebut.

Tujuan dan manfaat

- Langkah ini memungkinkan Anda untuk memahami setiap masalah yang mungkin ada.
- Dengan memahami masalah tersebut, Anda dapat menemukan tindakan spesifik yang harus dilakukan sebagai langkah selanjutnya.

Jika perusahaan Anda tidak menggunakan item

Beberapa item di bawah ini mungkin tidak berlaku untuk perusahaan Anda, bergantung pada jenis bisnisnya. Untuk kasus tersebut, lingkari “Diimplementasikan.”

- No. 4 Jaringan yang terhubung ke mesin fotokopi dan hard drive
- No. 5 Layanan web
- No. 9 LAN nirkabel
- No. 23 Layanan Cloud

Jika menurut Anda, “Kami tidak memiliki ‘informasi rahasia’ apa pun, item-item di bawah ini adalah materi rahasia!

- Alamat karyawan, dan slip gaji
- Daftar pembayaran untuk setiap mitra bisnis dan informasi transaksi
- Informasi akuntansi organisasi Anda
- Daftar kontak pelanggan dan mitra bisnis
- Informasi pengembangan seperti gambar desain untuk produk baru
- Setiap informasi dari mitra bisnis yang harus ditangani dengan hati-hati

Terdapat informasi yang harus dikelola sebagai informasi di antara berbagai informasi dasar suatu organisasi. Anda harus mengonfirmasi dan mengatur jenis informasi apa yang ada di perusahaan Anda yang bersifat rahasia. Klasifikasi data ini adalah langkah pertama dalam keamanan informasi.

2 Bacalah uraian berikut ini setelah melakukan penilaian.

Jika Anda mencetak 100 poin sempurna	Langkah keamanan dasar Anda sudah sempurna. Pikirkan tentang langkah Anda untuk naik ke level berikutnya.
Jika Anda mencetak 70-99 poin	Hampir sempurna, tetapi ada beberapa bidang dengan langkah yang belum lengkap.
Jika Anda mencetak 50-69 poin	Terdapat bidang yang secara eksplisit mengalami kekurangan langkah.
Jika Anda mencetak 49 poin atau lebih rendah	Anda seharusnya tidak terkejut jika ada insiden seperti kebocoran data.

Langkah yang dijelaskan dalam lembar Penilaian Mandiri Perusahaan didasarkan pada hal berikut.

- ■ Seorang pimpinan (perwakilan) dapat secara langsung menginstruksikan dan mengonfirmasi apakah langkah kebijakan telah diimplementasikan.
- ■ Semua karyawan saling mengenali.
- ■ Perusahaan tidak memiliki server atau peralatan jaringan yang memerlukan pengaturan rumit di perusahaan.
  - • Situs web perusahaan tidak menggunakan server yang terhubung langsung ke Internet, seperti menggunakan layanan cloud.
  - • Tidak ada perangkat lunak aplikasi yang dikembangkan oleh perusahaan, dan hanya menggunakan perangkat lunak aplikasi yang tersedia secara komersial.
  - • Komputer pribadi dapat digunakan untuk bekerja hanya jika langkah yang sama juga diterapkan pada komputer milik perusahaan.

Penilaian Mandiri

Lembar 5 Menit Penilaian Mandiri Perusahaan

Lembar penilaian mandiri perusahaan untuk mengidentifikasi langkah keamanan informasi yang harus Anda prioritaskan sebagai sebuah organisasi

- Silakan baca [1] di halaman sebelumnya sebelum melakukan penilaian ini.
- Bacalah item penilaian di bawah ini dan lingkari kolom yang sesuai.
- Lembar ini harus diisi oleh pejabat pimpinan atau manajer.
- Jawablah apakah item yang ditunjukkan dengan telah diimplementasikan oleh semua karyawan. Jika suatu item hanya diimplementasikan oleh beberapa karyawan, pilih "Diimplementasikan sebagian".
  Silakan jawab apakah item yang ditunjukkan oleh telah diimplementasikan oleh perusahaan Anda.
- Tambahkan skor Anda di bagian bawah halaman, lalu lanjutkan membaca [2] di halaman sebelumnya.

Organisasi: _____

Responden: _____

Tanggal: _____

Item penilaian	No.	Deskripsi	Tanggapan			
			Diimplementasikan	Diimplementasikan sebagian	Tidak diimplementasikan	Tidak tahu
Bagian 1 Langkah dasar	1	Apakah Anda selalu menjaga OS dan perangkat lunak Anda terlindungi dengan memperbarui Windows (Windows Update)*1 atau menggunakan langkah lain?	4	2	0	0
	2	Apakah Anda mengambil langkah untuk melindungi PC Anda dari virus, seperti menginstal perangkat lunak antivirus dan secara otomatis memperbarui file definisi virus?*2	4	2	0	0
	3	Sudahkah Anda membuat kata sandi yang kuat yang tidak mudah ditebak serta tidak menggunakan kata sandi seperti nama, nomor telepon, atau tanggal lahir, dan apakah Anda tidak menggunakan kata sandi yang sama untuk beberapa layanan web?	4	2	0	0
	4	Apakah Anda membatasi secara tepat akses ke informasi penting, seperti pembatasan dalam berbagi mesin fotokopi yang terhubung ke jaringan atau hard drive hanya untuk mereka yang membutuhkannya?	4	2	0	0
	5	Apakah Anda memiliki sistem untuk mengidentifikasi ancaman dan metode serangan baru, serta membaginya secara internal dengan memeriksa dan membagikan peringatan keamanan dari produsen produk atau layanan web*3 yang Anda gunakan?	4	2	0	0
Bagian 2 Langkah sebagai karyawan	6	Apakah Anda berhati-hati dengan email phishing, dan berupaya untuk tidak membuka lampiran dalam email yang mencurigakan atau mengeklik tautan dalam pesan?	4	2	0	0
	7	Apakah Anda memiliki sistem untuk memeriksa dan mencegah kesalahan pengiriman email, seperti dengan memeriksa alamat secara visual sebelum mengirim email?	4	2	0	0
	8	Apakah Anda melindungi informasi penting dengan melindungi lampiran menggunakan kata sandi atau langkah serupa lainnya sebelum mengirimnya melalui email?	4	2	0	0
	9	Apakah Anda mengambil langkah untuk mengamankan LAN nirkabel, seperti selalu mengimplementasikan enkripsi yang kuat saat menggunakannya?	4	2	0	0
	10	Apakah Anda mengambil langkah untuk mengontrol penggunaan Internet, seperti menetapkan aturan tentang menjelajahi situs web dan memposting ke media sosial di komputer kantor?	4	2	0	0
	11	Apakah Anda mengambil langkah untuk melakukan pencadangan rutin, guna mencegah agar informasi penting tidak hilang karena kegagalan fungsi atau kesalahan operasi?	4	2	0	0
	12	Apakah Anda mengambil langkah untuk mencegah hilang atau bocornya informasi penting, seperti menyimpan informasi penting di kabinet yang terkunci, dan tidak meninggalkannya di atas meja?	4	2	0	0
	13	Saat membawa informasi penting ke luar kantor, apakah Anda mengambil langkah untuk menghadapi risiko pencurian atau kehilangan, seperti melindunginya dengan kata sandi atau mengenkripsinya, serta menjaganya setiap saat?	4	2	0	0
	14	Apakah Anda mengambil langkah untuk memastikan orang lain tidak menggunakan komputer Anda, seperti mengatur layar kunci komputer saat meninggalkan meja kerja?	4	2	0	0
	15	Apakah Anda mencoba untuk mencegah orang yang tidak berwenang memasuki kantor dengan mendekati orang asing ketika Anda melihat seseorang yang tidak dikenal masuk ke kantor, atau dengan mengambil langkah lain?	4	2	0	0
	16	Apakah Anda mengambil langkah untuk mencegah pencurian saat meninggalkan kantor seharian, seperti mengunci laptop dan aksesori di laci, dan tidak meninggalkannya di atas meja?	4	2	0	0
	17	Apakah kunci kantor dikelola dengan cara yang benar, seperti memastikan orang terakhir yang meninggalkan kantor pada hari itu mengunci kantor dan mencatat (nama mereka, tanggal, dan jam)?	4	2	0	0
	18	Saat membuang informasi penting, apakah Anda mengambil langkah untuk membuat informasi penting menjadi tidak terbaca, seperti merobek dokumen atau menggunakan alat penghapus data?	4	2	0	0
Bagian 3 Langkah sebagai organisasi	19	Apakah Anda memiliki Kode Etik Karyawan untuk menjaga kerahasiaan, seperti memberi tahu karyawan saat direkrut bahwa mereka wajib menjaga kerahasiaan dan terdapat ketentuan hukuman?	4	2	0	0
	20	Apakah Anda mengadakan pelatihan kesadaran keamanan agar karyawan sadar akan pentingnya manajemen informasi, seperti dengan menjelaskan pentingnya hal tersebut secara rutin?	4	2	0	0
	21	Apakah Anda menjelaskan tentang boleh tidaknya karyawan menggunakan perangkat pribadi saat bekerja, seperti dengan menetapkan kebijakan tentang penggunaan komputer pribadi dan smartphone di dalam dan di luar perusahaan?	4	2	0	0
	22	Apakah Anda mewajibkan mitra bisnis untuk menjaga kerahasiaan, seperti menyertakan klausul kerahasiaan (kewajiban untuk menjaga kerahasiaan) dalam kontrak?	4	2	0	0
	23	Apakah Anda mengonfirmasi keamanan dan keandalan layanan dengan memeriksa syarat penggunaan dan langkah keamanan sebelum memilih layanan eksternal, seperti layanan cloud?	4	2	0	0
	24	Sudahkah persiapan dilakukan apabila terjadi insiden keamanan informasi, seperti menyusun prosedur tanggapan untuk kebocoran, kehilangan, atau pencurian informasi rahasia?	4	2	0	0
	25	Apakah Anda mendefinisikan konten langkah keamanan informasi, seperti menjadikan langkah keamanan informasi (seperti item 1 hingga 24 di atas) sebagai kebijakan perusahaan?	4	2	0	0

*1 Program yang disediakan oleh Microsoft Corporation yang memperbaiki kerusakan pada PC Windows

*2 File database yang disebut "pattern file" untuk mendeteksi virus komputer

*3 Nama umum layanan yang digunakan melalui Internet seperti Internet banking, media sosial, webmail, dan kalender

★ Tidak ada jaminan bahwa langkah-langkah yang dijelaskan dalam lembar Penilaian Mandiri Perusahaan dapat menawarkan perlindungan lengkap.

A	B	A+B
Total poin yang diimplementasikan	Total poin yang diimplementasikan sebagian	Skor
Poin	Poin	Poin

Penjelasan

Bagian 1 Langkah dasar

Item No. 1 hingga 5 adalah langkah yang harus diambil terlepas dari ukuran dan bentuk perusahaan. Peninjauan langkah ini secara berkelanjutan dan bukan hanya satu kali saja adalah hal hal pokok yang perlu dilakukan. Penerapannya sebagai peraturan perusahaan juga penting agar peraturan tersebut dapat dipatuhi oleh semua karyawan.

Pembaruan keamanan penting untuk dijadikan prioritas pertama!

Item No. 1 Langkah melindungi kerentanan

Selalu perbarui OS dan perangkat lunak Anda

Mengabaikan masalah keamanan pada OS dan perangkat lunak akan membuat perangkat Anda rentan terinfeksi virus berbahaya. Pastikan Anda mengimplementasikan *patch* pembaruan ke OS dan perangkat lunak Anda atau gunakan versi terbaru.

Tindakan Ambil langkah, seperti menggunakan Windows Update (OS Windows) atau menggunakan versi terbaru dari Adobe Flash Player, Adobe Reader, lingkungan runtime Java, dan perangkat lunak lainnya.

Item No. 2 Langkah antivirus

Instal perangkat lunak antivirus dan gunakan dengan tepat

Semakin banyak virus yang mencuri ID dan kata sandi, mengoperasikan komputer dari jarak jauh, dan mengenkripsi file secara tidak bertanggung jawab. Pastikan untuk menginstal perangkat lunak antivirus dan pastikan file definisi virus (pattern file) selalu terbarui.

Tindakan Ambil langkah, seperti mengatur perangkat Anda agar secara otomatis memperbarui file definisi virus dan pertimbangkanlah untuk menginstal perangkat lunak keamanan terkonsolidasi.

Item No. 3 Manajemen kata sandi

Gunakan kata sandi yang kuat

Terjadi peningkatan jumlah kerusakan akibat login yang tidak sah karena kata sandi yang mudah ditebak dan penggunaan berbahaya ID dan kata sandi secara tidak bertanggung jawab yang bocor dari layanan web. Buatlah kata sandi yang kuat dengan menjadikannya panjang dan rumit, dan jangan menggunakannya. berulang-kali di web yang berbeda

*Kata sandi sederhana: Kata sandi yang mudah ditebak oleh pihak ketiga, seperti nama Anda, nama perusahaan, atau kata-kata bahasa Inggris sederhana dalam kamus.

Tindakan Ambil langkah, seperti membuat kata sandi yang merupakan kombinasi dari 10 atau lebih karakter, angka, dan simbol. Jangan menggunakan nama, nomor telepon, tanggal lahir, dll., dan jangan gunakan kata sandi yang sama untuk beberapa layanan web dan situs web lain.

Item No. 4 Pengaturan perangkat

Tinjaulah pengaturan berbagi

Terjadi peningkatan kekhawatiran akan adanya kemungkinan orang yang tidak berwenang dapat melihat informasi dikarenakan data disimpan di server file atau penyimpanan online, atau mesin fotokopi jaringan yang tidak dikonfigurasi dengan benar. Pastikan server dan perangkat jaringan hanya dibagikan kepada orang yang memiliki izin untuk mengaksesnya.

Tindakan Ambil langkah, seperti membatasi cakupan berbagi layanan cloud, membatasi cakupan berbagi perangkat yang terhubung dengan jaringan, dan mengubah pengaturan ketika karyawan pindah ke departemen lain atau pensiun.

Item No. 5 Pengumpulan informasi

Pelajari metode ancaman dan serangan dan ambil langkah untuk menghadapinya.

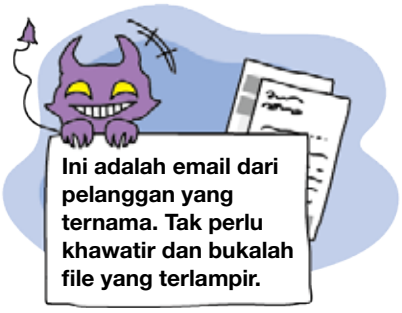
Terjadi peningkatan jumlah serangan *phishing* untuk mencuri ID dan kata sandi melalui email dengan virus yang menyamar sebagai mitra bisnis atau pemangku kepentingan lainnya, atau mengarahkan seseorang untuk membuka situs web palsu yang meniru situs web yang sah. Ambil langkah untuk menghadapi metode ancaman dan serangan dengan cara mempelajarinya terlebih dahulu.

Tindakan Ambil langkah, seperti memeriksa situs web IPA dan berlangganan majalah untuk mempelajari metode ancaman dan serangan terbaru, serta mengonfirmasi peringatan yang diberikan oleh layanan Internet banking dan layanan lain yang digunakan.

Bagian 2

Langkah sebagai karyawan

Item No. 6 hingga 18 adalah item yang harus diperhatikan karyawan. Kesalahan manusia dapat dengan mudah terjadi karena mereka terbiasa menangani informasi penting setiap hari dan disebabkan oleh kelalaian. Selain itu, sifat ancaman yang berubah setiap hari mengharuskan Anda untuk selalu waspada.



Item No. 6 Aturan email

Berhati-hatilah terhadap setiap email yang diterima dari seseorang yang tidak Anda kenal

Email tersebut dapat menyebarkan virus apabila Anda membuka lampiran email atau mengeklik tautan URL di badan email. Waspadalah dengan lampiran dan jangan mudah mengeklik tautan URL dari pengirim yang tidak Anda kenal.

Tindakan **Ambil langkah, seperti tidak membuka lampiran atau mengeklik tautan URL di email yang mencurigakan, dan melaporkan email mencurigakan ke departemen keamanan Anda untuk membagikan informasi tentang email mencurigakan di perusahaan.**

Item No. 7 Aturan email

Hindari mengirim email ke penerima yang salah

Terdapat potensi insiden bocornya informasi kepada orang asing apabila Anda keliru mengirimkan email atau faksimile ke orang yang salah. Pastikan untuk memeriksa penerima email dan faks dengan cermat. Selain itu, kebocoran informasi juga dapat terjadi ketika Anda secara tidak sengaja memberikan alamat email yang salah kepada seseorang. Saat mengirim email ke beberapa orang, pastikan Anda memvalidasi alamat penerima.

Tindakan **Ambil langkah, seperti mengecek alamat sebelum mengirim email atau faksimile, dan pilih alamat To, CC, dan BCC dalam email tersebut secara terpisah.**

Item No. 8 Aturan email

Lindungi informasi penting saat mengirim email

Saat mengirim informasi penting melalui email, jangan menuliskannya di badan email. Namun tulislah dalam suatu file, lindungi dengan kata sandi, dan lampirkan file ke email. Beri tahukan kata sandi kepada penerima email dengan menelepon mereka atau dengan cara lain, bukan menuliskannya di email.

Tindakan **Ambil langkah, seperti menulis informasi penting dalam file dan melindunginya dengan kata sandi. Beri tahukan kata sandi kepada penerima email melalui telepon atau dengan cara lain.**

Item No. 9 Aturan LAN Nirkabel

Cegahlah penyadapan dan penggunaan LAN nirkabel tanpa izin

LAN nirkabel yang tidak memiliki pengaturan keamanan yang memadai berpotensi mengalami kebocoran atau penyalahgunaan data untuk tindakan kriminal dengan menghubungkannya secara ilegal ke pencuri data. Pastikan untuk mengatur keamanan LAN nirkabel guna mencegah penyadapan dan penggunaan yang tidak sah.

Tindakan **Ambil langkah, seperti menggunakan pengaturan enkripsi (mis. WPA2-PSK) dan menggunakan frase sandi yang panjang dan sulit ditebak.**

Item No. 10 Aturan penggunaan internet

Cegahlah masalah saat menggunakan Internet

Melihat situs web berbahaya atau situs web dengan masalah keamanan dapat menyebabkan perangkat Anda terinfeksi virus. Selain itu, perusahaan juga dapat dirugikan oleh lelucon nyata yang dikirim di media sosial maupun papan pesan, atau oleh informasi rahasia yang dikirim tanpa disengaja. Pencegahan bahaya penting untuk dilakukan dengan mengimplementasikan sistem dan aturan yang membatasi penggunaan Internet di tempat kerja.

Tindakan **Ambil langkah, seperti membuat aturan akses untuk menggunakan Internet dan media sosial, dan gunakan filter web untuk secara sistematis membatasi penggunaan Internet.**

Item No. 11 Aturan pencadangan

Giatkanlah tindakan pencadangan rutin

Data yang disimpan pada PC atau server dapat hilang akibat kegagalan fungsi, kesalahan operasi, atau infeksi virus. Buatlah cadangan data untuk mengantisipasi situasi tidak terduga semacam itu.

Tindakan **Ambil langkah, seperti melakukan pencadangan informasi penting secara rutin dan menyimpan cadangan di lokasi terpisah.**

Penjelasan

Item No. 12 Pengaturan penyimpanan

Informasi/dokumen penting harus ditangani dengan benar

Meninggalkan informasi/dokumen tanpa pengawasan di atas meja adalah tindakan berbahaya karena dapat diambil atau dibaca oleh seseorang. Informasi/dokumen penting harus ditangani dengan benar untuk mencegah orang lain melihat atau menyentuhnya, serta memastikan informasi/dokumen berada dalam pengawasan. Tentukan lokasi penyimpanan informasi/dokumen. Keluarkan informasi/dokumen hanya jika diperlukan untuk bekerja, dan pastikan untuk menyimpannya kembali setelah selesai.

Tindakan

Ambil langkah, seperti menjaga meja tetap rapi dan tertata, serta menyimpan informasi/dokumen penting dalam kabinet yang terkunci.

Item No. 13 Aturan membawa informasi penting

Bawalah informasi penting dengan cara yang aman

Ketika membawa informasi penting di luar perusahaan, ada potensi informasi tersebut dicuri atau hilang. Ambil langkah terlebih dahulu saat menggunakan laptop atau smartphone, seperti mengatur kata sandi atau mengenkripsi file data, sehingga informasi tersebut tidak dengan mudah dilihat jika dicuri atau hilang.

Tindakan

Ambil langkah, seperti mewajibkan adanya izin terlebih dahulu untuk membawa informasi penting, mengamankan data dengan kata sandi pada laptop, smartphone, dan stik USB, dan tidak meninggalkan bagasi tanpa pengawasan.

Item No. 14 Manajemen keamanan kantor

Jangan biarkan siapa pun menggunakan perangkat tanpa izin

Jangan tinggalkan komputer tanpa pengawasan selama jam kerja. PC tanpa pengawasan yang dapat dioperasikan oleh siapa saja, seperti yang dapat dimasuki tanpa kata sandi, dapat disalahgunakan. Ambil langkah untuk melindungi PC agar tidak digunakan secara tidak sah.

Tindakan

Ambil langkah, seperti mengunci PC ketika meninggalkan meja, mematikan PC ketika meninggalkan kantor pada hari tersebut, dan mencegah orang lain menggunakan PC Anda.

Item No. 15 Manajemen keamanan kantor

Dekatilah orang yang tidak Anda kenal

Terdapat potensi bahaya pencurian informasi jika Anda tidak membatasi akses bagi orang yang tidak berwenang untuk memasuki kantor. Pastikan bahwa orang yang tidak berwenang tidak diizinkan untuk mengakses lokasi penyimpanan informasi/dokumen penting, terutama seperti server, arsip, dan brankas.

Tindakan

Ambil langkah, seperti mendekati seseorang yang tidak Anda kenal di kantor atau menyiapkan meja resepsionis.

Item No. 16 Manajemen keamanan kantor

Ambillah langkah untuk mencegah pencurian peralatan dan aksesori

Meskipun perangkat seperti komputer laptop, tablet, dan stik USB kini makin nyaman dan ringkas, hal ini juga berpotensi meningkatkan risiko pencurian perangkat tersebut. Saat perangkat tidak digunakan, ambil langkah untuk menyimpannya di tempat yang aman, seperti di laci yang dapat dikunci.

Tindakan

Ambil langkah, seperti mengunci laptop, tablet, dan aksesori (CD, stik USB, *hard drive* eksternal, dll.) di laci meja ketika meninggalkan kantor pada hari tersebut.

Item No. 17 Manajemen keamanan kantor

Bersikaplah waspada saat mengunci pintu kantor

Mencatat waktu bagi orang yang terakhir keluar dari kantor juga membantu meningkatkan rasa tanggung jawab pada orang yang terakhir mengunci pintu. Berusahalah mengelola kunci dan catatan.

Tindakan

Ambil langkah, seperti mengelola kunci dan mencatat orang terakhir di kantor yang mengunci pintu (tanggal, jam, dan nama).

Item No. 18 Pemusnahan/penghapusan informasi yang aman

Hapuslah informasi penting sehingga informasi tersebut tidak dapat dipulihkan

Hanya dengan membuang dokumen berisi informasi penting ke tempat sampah dapat menyebabkan kebocoran informasi serius karena orang lain akan dapat membaca dokumen tersebut. Selain itu, informasi yang disimpan pada perangkat elektronik dan media elektronik juga dapat dipulihkan, meskipun file sudah dihapus. Saat memusnahkan informasi penting, musnahkan setiap bentuk informasi dengan tepat, seperti dengan menggunakan mesin penghancur kertas atau perangkat lunak penghapus data.

Tindakan

Ambil langkah untuk memusnahkan informasi, seperti dengan menggunakan perangkat lunak penghapus data, menghancurkannya secara fisik, atau meminta seorang spesialis untuk menghapusnya.

Simpan dokumen yang berisi informasi penting di dalam laci yang terkunci

Cegah pencurian perangkat

Kunci pintu kantor

Bagian 3

Langkah untuk organisasi

Item No. 19 hingga 25 adalah langkah yang harus diambil setelah menetapkan kebijakan untuk organisasi. Tingkatkan kesadaran karyawan dengan mendokumentasikan aturan keamanan informasi dengan jelas dan membagikannya di kantor.

Item No. 19 Menginformasikan kewajiban karyawan untuk menjaga kerahasiaan

Berilah pemahaman kepada karyawan tentang kewajiban mereka untuk menjaga kerahasiaan

Meskipun dapat dikatakan bahwa peraturan perusahaan telah mewajibkan karyawan untuk menjaga kerahasiaan dalam pekerjaan mereka, namun ada baiknya untuk memberi tahu karyawan tentang peraturan perusahaan yang harus diikuti secara jelas.

Tindakan Ambil langkah, seperti memberi tahu karyawan tentang kewajiban mereka untuk menjaga kerahasiaan ketika mereka direkrut.

Item No. 20 Pelatihan karyawan

Lakukan pelatihan karyawan secara rutin

Karyawan menangani informasi setiap hari dalam pekerjaan mereka, dan kebiasaan ini cenderung akan memunculkan kelalaian dan mereka mungkin lupa untuk mengelola informasi dengan aman. Pelatihan karyawan secara rutin akan efektif untuk meningkatkan kesadaran karyawan.

Tindakan Ambil langkah, seperti secara rutin menjelaskan pentingnya mengelola informasi serta melakukan pelatihan di kantor.

Item No. 21 Penggunaan perangkat pribadi

Putuskan apakah perusahaan akan mengizinkan penggunaan perangkat pribadi untuk bekerja

Memastikan keamanan menjadi sulit dilakukan jika perangkat pribadi seperti PC dan ponsel pintar digunakan untuk bekerja, karena pengelolaan tentang bagaimana karyawan menggunakannya tidak akan mudah. Putuskan apakah perangkat pribadi dapat digunakan untuk bekerja dan lakukan upaya untuk menetapkan aturan tentang penggunaannya.

Tindakan Ambil langkah, seperti membuat sistem perizinan untuk menggunakan perangkat pribadi seperti PC dan ponsel pintar untuk bekerja, serta tentukan aturan untuk penggunaannya jika hal tersebut diizinkan.

Item No. 22 Manajemen mitra bisnis

Mintalah mitra bisnis menjaga kerahasiaan

Hindari anggapan bahwa mitra bisnis pasti akan menjaga kerahasiaan berdasarkan sifat informasinya. Ketika memberikan informasi rahasia kepada mitra bisnis, perlu dijelaskan bahwa informasi tersebut harus diperlakukan sebagai rahasia.

Tindakan Ambil langkah, seperti menyusun kontrak yang menjelaskan bahwa konten harus diperlakukan sebagai rahasia.

Item No. 23 Penggunaan layanan eksternal

Gunakan layanan eksternal yang tepercaya

Jika memilih layanan eksternal, seperti layanan cloud, dengan prioritas biaya, Anda mungkin mendapati bahwa layanan mungkin tidak tersedia karena kegagalan dan masalah lainnya. Periksa kinerja, keandalan, perincian kompensasi, dan pertimbangan terkait lainnya secara menyeluruh saat menggunakan layanan eksternal untuk aplikasi yang memiliki dampak signifikan terhadap kelangsungan bisnis.

Tindakan Ambil langkah, seperti memeriksa persyaratan layanan, perincian kompensasi, langkah keamanan, dan hal lain yang relevan ketika memilih penyedia jasa.

Penjelasan

Item No. 24	Persiapan menghadapi insiden keamanan informasi

Persiapkan langkah untuk menghadapi insiden keamanan informasi

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. Gunakan insiden yang pernah dilaporkan di media sebagai referensi untuk memikirkan siapa dan kapan akan melakukan apa, dengan asumsi bahwa hal yang sama dapat terjadi di perusahaan Anda.

Tindakan	**Ambil langkah, seperti menyiapkan pedoman tanggapan untuk informasi penting yang bocor, hilang, atau dicuri.**

Item No. 25	Menyiapkan aturan

Buatlah aturan untuk langkah keamanan informasi

Meskipun pejabat pimpinan telah menetapkan kebijakan tentang langkah keamanan informasi, kecuali jika kebijakan secara jelas didokumentasikan sebagai aturan internal, karyawan harus selalu meminta saran dari manajer mereka. Agar karyawan dapat bertindak mandiri sesuai dengan aturan, pendokumentasian "aturan perusahaan" secara jelas sangatlah penting sehingga karyawan dapat merujuk pada kebijakan tersebut kapan saja.

Tindakan	**Ambil langkah, seperti membuat item dari lembar penilaian No. 1-24 sebagai aturan untuk langkah keamanan informasi kemudian membagikannya di perusahaan serta meninjau aturan ini secara rutin guna memperbaikinya jika terdapat kekurangan.**

NISC National center of Incident readiness and Strategy for Cybersecurity

BADAN SIBER DAN SANDI NEGARA BSSN

IPA Information-technology Promotion Agency, Japan

2019.04