Untuk PKS

Penilaian Kendiri
5 Minit
Keselamatan Maklumat

Adakah anda bersedia menghadapi ancaman keselamatan siber?

Perkembangan ancaman dan serangan

- *Ransomware*
- *Password list attacks*
- *Targeted e-mail attacks*

Perubahan dalam persekitaran IT

- Teknologi Awan
- Tablet
- Telefon pintar

Gunakan **"Soal Selidik Penilaian Kendiri 5 Minit"** ini untuk menyemak tahap keselamatan maklumat syarikat anda bagi mengelakkan sebarang kerugian!

ASEAN · JAPAN
Cybersecurity Cooperation

Penilaian Kendiri

1 Sila baca sebelum melaksanakan penilaian.

Latar belakang

Soal selidik ini memberi tumpuan kepada 25 langkah keselamatan maklumat yang berkesan dan mampu dilaksanakan oleh PKS. Soal selidik ini dapat membantu anda menyemak jika langkah-langkah tersebut telah dilaksanakan oleh syarikat anda. Jika terdapat langkah yang belum dilaksanakan, anda boleh merujuk kepada seksyen "Penerangan dan Tindakan Disyorkan" di dalam risalah ini sebagai panduan.

Faedah kepada anda

- Soal selidik ini membolehkan anda mengenal pasti ancaman keselamatan maklumat yang mungkin wujud di dalam syarikat anda.
- Dengan mengenal pasti ancaman, tindakan yang tepat dapat ditentukan untuk menanganinya.

Cara menjawab soal selidik

Sila jawab setiap soalan berdasarkan kepada keadaan semasa syarikat anda dan rujuk seksyen "Penerangan dan Tindakan Disyorkan" jika anda tidak memahami kehendak soalan tersebut.

Jika syarikat anda tidak menggunakan peranti atau perkhidmatan

Beberapa peranti/perkhidmatan berikut mungkin tidak digunakan oleh syarikat anda bergantung kepada jenis perniagaan. Dalam keadaan ini, sila pilih "Dilaksanakan" sebagai maklum balas anda.

- No.4 *Network connected photocopy machines and hard drives*
- No.5 Perkhidmatan web
- No.9 Wayarles LAN
- No.23 Perkhidmatan awan

Jika anda fikir, "Kami tidak mempunyai sebarang 'maklumat sulit', dokumen berikut adalah sulit!

- Alamat pekerja, dan slip gaji
- Senarai bayaran bagi setiap rakan kongsi perniagaan dan maklumat transaksi
- Maklumat perakaunan
- Senarai maklumat perhubungan bagi rakan kongsi perniagaan dan pelanggan
- Maklumat R&D seperti lukisan reka bentuk bagi produk baharu
- Maklumat sulit daripada rakan kongsi perniagaan

Terdapat maklumat yang perlu diklasifikasikan sebagai sulit di dalam maklumat asas sesebuah organisasi. Anda mestilah menentukan jenis-jenis maklumat dalam syarikat yang boleh dianggap sebagai sulit. Pengelasan data ini adalah langkah pertama dalam keselamatan maklumat.

2 Skala Markah: Sila rujuk selepas melaksanakan soal selidik

Jika anda mendapat 100 mata sempurna	Langkah-langkah keselamatan asas anda telah sempurna. Seterusnya, anda boleh membuat pertimbangan untuk menambah baik langkah-langkah tersebut.
Jika anda mendapat 70-99 mata	Hampir sempurna tetapi terdapat beberapa bidang yang mempunyai langkah kawalan yang tidak lengkap.
Jika anda mendapat 50-69 mata	Terdapat bidang yang jelas mempunyai langkah kawalan yang tidak mencukupi.
Jika anda mendapat 49 mata atau lebih rendah	Anda tidak seharusnya terkejut jika terdapat insiden seperti kebocoran data yang boleh berlaku pada bila-bila masa.

Seksyen "Penerangan dan Tindakan Disyorkan" ditulis berdasarkan andaian berikut:

- Seorang eksekutif boleh mengesahkan secara langsung sama ada langkah-langkah keselamatan maklumat yang dinyatakan telah dilaksanakan.
- Semua pekerja mengenali antara satu sama lain.
- Syarikat tidak memiliki pelayan atau peralatan rangkaian yang memerlukan tetapan rumit di dalam premis syarikat.
  - Syarikat tidak mempunyai web server sendiri tetapi menggunakan perkhidmatan awan
  - Syarikat tidak membangunkan aplikasi sendiri dan hanya menggunakan perisian/perkhidmatan yang tersedia secara komersial.
  - Komputer milik peribadi hanya dibenar untuk digunakan bagi urusan kerja jika langkah-langkah kawalan yang sama bagi komputer milik syarikat dilaksanakan ke atasnya

Penilaian Kendiri

Soal Selidik Penilaian Kendiri 5 Minit Syarikat

Helaian penilaian kendiri syarikat untuk mengenal pasti langkah-langkah keselamatan maklumat yang harus anda utamakan sebagai organisasi.

- Sila baca seksyen [1] pada halaman sebelumnya sebelum melakukan penilaian ini.
- Baca soal selidik berikut dan pilih maklum balas anda.
- Soal Selidik ini seharusnya diisi oleh eksekutif atau pengurus.
- Sila jawab sama ada item yang ditandakan dengan dilaksanakan oleh semua pekerja. Jika dilaksanakan oleh beberapa pekerja sahaja, pilih maklum balas "Dilaksanakan sebahagian." Sila jawab sama ada item yang ditandakan dengan dilaksanakan oleh syarikat anda.
- Jumlahkan markah anda di bahagian bawah halaman, dan rujuk [2] di halaman sebelumnya.

Nama: _____

Syarikat: _____

Tarikh: _____

Kategori	Item No.	Soalan	Maklum Balas			
			Dilaksanakan	Dilaksanakan Sebahagian	Tidak Dilaksanakan	Tidak tahu
Bahagian 1 Langkah-Langkah Asas	1	Adakah anda sentiasa memastikan OS dan perisian anda selamat, contohnya dengan mengemaskini Windows (Windows Update)*1?	4	2	0	0
	2	Adakah anda mengambil langkah untuk melindungi PC anda daripada virus, seperti memasang perisian antivirus dan mengemaskini fail definisi virus secara automatik?*2	4	2	0	0
	3	Adakah anda telah menetapkan kata laluan kukuh (tidak mudah diteka, tidak menggunakan nama, nombor telefon, atau tarikh lahir) dan tidak menggunakan kata laluan yang sama untuk pelbagai perkhidmatan web?	4	2	0	0
	4	Adakah anda mengehadkan akses dengan sewajarnya terhadap maklumat penting, seperti mengehadkan perkongsian *network connected photocopy machines dan hard drives* hanya kepada mereka yang memerlukannya?	4	2	0	0
	5	Adakah anda mempunyai sistem untuk mengenalpasti ancaman dan kaedah serangan baharu dan berkongsi secara dalaman dengan menyemak dan menyebarkan amaran keselamatan dari pengeluar produk atau perkhidmatan web*3 yang anda gunakan?	4	2	0	0
Bahagian 2 Tindakan Pekerja	6	Adakah anda berhati-hati dengan emel phishing, contohnya tidak membuka lampiran atau klik pautan di dalam emel yang mencurigakan?	4	2	0	0
	7	Adakah anda mempunyai sistem untuk menyemak dan menghalang penghantaran emel yang salah, seperti menyemak alamat secara visual sebelum menghantar emel?	4	2	0	0
	8	Adakah anda melindungi maklumat penting dengan meletakkan kata laluan pada lampiran atau menggunakan langkah lain yang serupa sebelum menghantar maklumat tersebut melalui emel?	4	2	0	0
	9	Adakah anda mengambil langkah untuk melindungi wayarles LAN anda, seperti sentiasa melaksanakan penyulitan yang kuat apabila menggunakannya?	4	2	0	0
	10	Adakah anda mengambil langkah untuk mengawal penggunaan Internet, seperti menetapkan peraturan dalam melayari laman web dan media sosial menggunakan komputer pejabat?	4	2	0	0
	11	Adakah anda mengambil langkah untuk mengelakkan kehilangan data akibat kerosakan atau ralat operasi, contohnya melaksanakan sandaran dengan kerap (regular backup)?	4	2	0	0
	12	Adakah anda mengambil langkah untuk mengelakkan kehilangan atau kebocoran maklumat penting, seperti menyimpannya di dalam kabinet berkunci berbanding meninggalkannya di atas meja?	4	2	0	0
	13	Apabila membawa maklumat penting keluar daripada pejabat, adakah anda mengambil langkah-langkah mengelakkan kecurian atau kehilangan, seperti melindunginya dengan kata laluan atau menyulitkannya dan menyimpannya bersama anda pada setiap masa?	4	2	0	0
	14	Adakah anda mengambil langkah untuk memastikan orang lain tidak menggunakan komputer anda, seperti menetapkan skrin kunci (lock screen) komputer apabila anda meninggalkan meja anda?	4	2	0	0
	15	Adakah anda menghalang orang tanpa kebenaran daripada memasuki pejabat, contohnyam anda menghampiri dan menegur seseorang yang tidak dikenali apabila menyedari kehadirannya di pejabat anda?	4	2	0	0
	16	Adakah anda mengambil langkah untuk menghalang kecurian apabila meninggalkan pejabat setiap hari, seperti mengunci komputer riba dan aksesori di dalam laci berbanding meninggalkannya di atas meja?	4	2	0	0
	17	Adakah kunci pejabat diurus dengan cara yang betul, contohnya, orang terakhir yang meninggalkan pejabat mengunci pejabat dan merekodkan dalam buku log (nama, tarikh dan masa)?	4	2	0	0
	18	Apabila melupuskan maklumat penting, adakah anda mengambil langkah untuk menjadikan maklumat penting itu tidak boleh dibaca, seperti merincih dokumen atau menggunakan alat memadam data?	4	2	0	0
Bahagian 3 Pengurusan Organisasi	19	Adakah anda memastikan para pekerja menguruskan maklumat sulit dengan baik, contohnya dengan memaklumkan pekerja apabila mereka dilantik bahawa mereka diwajibkan untuk mengekalkan kerahsiaan maklumat dan terdapat peruntukan untuk hukuman jika ingkar?	4	2	0	0
	20	Adakah anda melaksanakan latihan kesedaran keselamatan untuk memastikan pekerja sedar mengenai kepentingan pengurusan maklumat, seperti menerangkan kepentingannya secara kerap?	4	2	0	0
	21	Adakah anda menjelaskan sama ada pekerja boleh menggunakan peranti peribadi dalam kerja mereka, seperti menetapkan polisi bagi penggunaan komputer peribadi dan telefon pintar di dalam dan di luar syarikat?	4	2	0	0
	22	Adakah anda memerlukan rakan kongsi mengekalkan kerahsiaan, seperti menyertakan fasal kerahsiaan (kewajipan untuk mengekalkan kerahsiaan) dalam kontrak?	4	2	0	0
	23	Adakah anda mengesahkan keselamatan dan kebolehpercayaan perkhidmatan dengan menyemak terma penggunaan dan langkah-langkah keselamatan sebelum memilih perkhidmatan luaran, seperti perkhidmatan awan?	4	2	0	0
	24	Adakah persediaan telah dilakukan sekiranya berlaku insiden keselamatan maklumat, seperti merangka prosedur tindak balas untuk kebocoran, kehilangan, atau kecurian maklumat sulit?	4	2	0	0
	25	Adakah anda menetapkan kandungan langkah-langkah keselamatan maklumat, contohnya, menjadikan langkah-langkah keselamatan maklumat (seperti item 1 hingga 24 di atas) sebagai polisi syarikat?	4	2	0	0

*1 Program yang disediakan oleh Microsoft Corporation yang membetulkan kecacatan pada perisian Windows

*2 Fail pangkalan data yang dipanggil "pattern file" untuk mengesan virus komputer

*3 Nama umum bagi perkhidmatan yang digunakan melalui Internet seperti perbankan Internet, media sosial, emel, dan kalendar

★ Tiada jaminan bahawa langkah-langkah yang diterangkan di helaian Penilaian Kendiri Syarikat menawarkan perlindungan lengkap.

A Jumlah markah dilaksanakan	B Jumlah markah dilaksanakan sebahagian	A+B Markah Keseluruhan
Markah	Markah	Markah

Penerangan dan Tindakan Disyorkan

Bahagian 1 Langkah-Langkah Asas

Item No 1 hingga 5 adalah langkah asas yang perlu diambil tanpa mengambil kira saiz dan bentuk syarikat. Langkah-langkah ini perlu disemak secara berterusan dan bukan hanya dilaksanakan sekali sahaja. Langkah-langkah ini perlu dijadikan sebagai peraturan syarikat untuk dipatuhi oleh semua pekerja.

PENTING: Pastikan bahawa keselamatan adalah keutamaan syarikat anda!!

Item No 1 — Tampung Kerentanan (*Vulnerability Patches*)

Sentiasa pastikan OS dan perisian anda adalah versi terkini

Mengabaikan isu keselamatan OS dan perisian anda menjadikan peranti anda mudah dijangkiti oleh virus. Pastikan untuk melaksanakan kemaskini OS dan perisian anda atau gunakan versi terkini.

Tindakan — Ambil langkah, seperti menggunakan Windows Update atau menggunakan versi terkini Adobe Flash Player, Adobe Reader, Java Runtime Environment, dan perisian lain.

Item No 2 — Perisian antivirus

Pasang perisian antivirus dan gunakan sewajarnya

Terdapat virus yang yang mampu mencuri ID dan kata laluan, mengendalikan komputer secara kawalan jauh, dan menyulitkan fail sewenang-wenangnya. Pastikan untuk memasang perisian antivirus dan pastikan bahawa fail definisi virus (pattern file) sentiasa terkemaskini.

Tindakan — Ambil langkah, seperti menetapkan peranti anda untuk mengemaskini fail definisi virus secara automatik dan pertimbangkan untuk memasang *consolidated security software*.

Item No 3 — Pengurusan kata laluan

Gunakan kata laluan yang kukuh

Log masuk tanpa kebenaran boleh berlaku jika menggunakan kata laluan yang mudah diteka. Gunakan kata laluan anda kukuh dengan menjadikannya panjang, rumit dan tidak menggunakan kata laluan yang sama untuk pelbagai sistem/perkhidmatan web.

*Kata laluan mudah: Kata laluan yang mudah diteka oleh pihak ketiga, seperti nama anda, nama syarikat atau perkataan Bahasa Inggeris mudah di dalam kamus.

Tindakan — Ambil langkah, seperti menjadikan kata laluan kombinasi 10 atau lebih aksara, nombor, dan simbol. Jangan gunakan nama, nombor telefon, tarikh lahir, dll., dan jangan gunakan kata laluan yang sama untuk perkhidmatan web dan laman web berlainan.

Item No 4 — Tetapan peranti

Semak semula tetapan kawalan akses

Kebocoran maklumat boleh berlaku apabila orang yang tiada kebenaran dapat mengakses maklumat atau data yang disimpan pada pelayan fail, storan atas talian, atau mesin penyalin rangkaian yang dikonfigurasikan secara salah. Pastikan bahawa pelayan dan peranti rangkaian hanya boleh diakses oleh orang yang dibenarkan sahaja.

Tindakan — Ambil langkah, seperti mengehadkan skop bagi perkongsian perkhidmatan awan, mengehadkan skop perkongsian peranti sambungan rangkaian, dan menukar tetapan apabila pekerja berpindah ke jabatan lain atau bersara.

Item No 5 — Ancaman

Belajar mengenai kaedah serangan dan ancaman dan ambil langkah untuk melawannya.

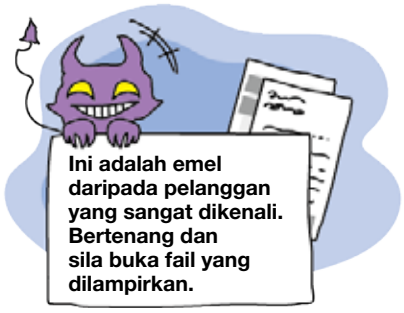
Terdapat peningkatan jumlah serangan memancing data (phishing) untuk mencuri ID dan kata laluan melalui emel menggunakan virus yang menyamar sebagai rakan kongsi perniagaan atau lembaga pengarah lain, atau membawa orang ke laman web penipuan yang meniru laman web yang sah. Ambil langkah untuk melawan kaedah serangan dan ancaman dengan belajar mengenainya.

Tindakan — Ambil langkah, seperti menyemak laman web vendor keselamatan dan melanggan majalah emel untuk belajar mengenai kaedah serangan dan ancaman terkini, dan mengesahkan amaran yang disediakan oleh perbankan Internet dan perkhidmatan lain yang digunakan.

Penerangan dan Tindakan Disyorkan

Bahagian 2 Peranan pekerja

Item No 6 hingga 18 adalah langkah yang sepatutnya dilaksanakan oleh setiap pekerja. Kesilapan manusia mudah berlaku disebabkan oleh kebiasaan pengendalian maklumat penting setiap hari. Anda perlu berhati-hati pada setiap masa kerana sifat ancaman yang berubah dari hari ke hari.



Item No 6 | Emel

Berjaga-jaga terhadap sebarang emel yang diterima daripada seseorang yang tidak dikenali

Membuka lampiran atau klik pada pautan di dalam emel yang mecurigakan boleh menyebabkan jangkitan virus. Berhati-hati dengan lampiran dan pautan URL daripada penghantar yang tidak dikenali.

Tindakan — **Ambil langkah, seperti tidak membuka lampiran atau pautan URL di dalam emel yang mencurigakan, dan laporkan sebarang emel yang mencurigakan kepada jabatan keselamatan untuk berkongsi maklumat mengenai emel yang mencurigakan dalam syarikat.**

Item No 7 | Emel

Elak menghantar emel kepada penerima yang salah

Kebocoran maklumat boleh berlaku apabila anda menghantar emel atau faks kepada alamat emel atau nombor faks yang silap. Pastikan anda menyemak dengan betul penerima emel dan faks anda. Kebocoran maklumat juga berlaku apabila anda memberi alamat emel yang salah kepada seseorang. Apabila menghantar emel kepada beberapa penerima, pastikan untuk menyemak alamat penerima.

Tindakan — **Ambil langkah, seperti semak alamat dua kali sebelum menghantar emel atau faks, dan memilih alamat Kepada, CC dan BCC secara berasingan di dalam emel.**

Item No 8 | Emel

Lindungi maklumat penting yang dihantar melalui emel

Jika ingin menghantar maklumat penting melalui emel, jadikannya sebagai dokumen lampiran dan lindungi dengan kata laluan. Maklumkan kata laluan kepada penerima emel melalui telefon atau cara lain selain emel.

Tindakan — **Ambil langkah, seperti menulis maklumat penting di dalam fail dan melindunginya dengan kata laluan. Maklumkan penerima mengenai kata laluan melalui telefon atau melalui cara lain.**

Item No 9 | Wayarles LAN

Elakkan curi dengar dan penggunaan tanpa kebenaran bagi wayarles LAN.

Wayarles LAN yang tidak mempunyai tetapan keselamatan yang mencukupi mungkin terdedah kepada kebocoran data atau penyalahgunaan untuk tujuan jenayah dengan menyambungnya secara haram. Pastikan untuk menetapkan keselamatan wayarles LAN bagi menghalang perbuatan curi dengar dan penggunaan tanpa kebenaran.

Tindakan — **Ambil langkah, seperti menggunakan tetapan penyulitan (cth. WPA2-PSK) dan menggunakan kata laluan yang panjang dan sukar diteka.**

Item No 10 | Penggunaan Internet

Kawal penggunaan Internet

Penggunaan Internet yang tidak dikawal boleh menjejaskan keselamatan jika melayari laman web yang tidak selamat. Kawal dan hadkan akses Internet hanya untuk tujuan kerja.

Tindakan — **Ambil langkah, seperti mewujudkan peraturan akses untuk menggunakan Internet dan media sosial, dan menggunakan web filters untuk mengehadkan penggunaan Internet secara sistematik.**

Item No 11 | Sandaran (*Backup*)

Laksanakan sandaran data secara berkala

Data yang disimpan pada PC atau pelayan boleh hilang disebabkan oleh kerosakan, salah operasi, atau jangkitan virus. Lakukan sandaran data untuk bersedia bagi situasi tidak dijangka tersebut.

Tindakan — **Ambil langkah, seperti melakukan sandaran bagi maklumat penting secara tetap dan menyimpan sandaran di lokasi berbeza.**

Penerangan dan Tindakan Disyorkan

Item No 12 | Penyimpanan/Storan

Maklumat/dokumen penting mestilah dikendalikan dengan betul

Maklumat/dokumen penting mestilah dikendalikan dengan betul untuk menghalang orang lain daripada melihat atau mengaksesnya dan pastikan bahawa ia tidak ditinggalkan tanpa pengawasan. Tetapkan lokasi penyimpanan untuk maklumat/dokumen, ambil ia keluar apabila perlu untuk kerja sahaja, dan pastikan untuk menyimpannya semula apabila selesai.

Tindakan — **Ambil langkah, seperti memastikan meja kemas dan rapi, dan menyimpan maklumat/dokumen penting di dalam kabinet berkunci.**

Item No 13 | Pergerakan Maklumat

Pindahkan maklumat penting dengan cara selamat

Apabila membawa maklumat penting ke luar daripada syarikat, kecurian boleh berlaku tanpa disangka atau hilang secara tidak sengaja. Ambil langkah awal apabila menggunakan komputer riba atau telefon pintar, seperti menetapkan kata laluan atau menyulitkan fail data, supaya maklumat tidak mudah dilihat sekiranya ia dicuri atau hilang.

Tindakan — **Ambil langkah, seperti menjadikannya wajib untuk mendapatkan kebenaran sebelum memindahkan maklumat penting, melindungi data dengan kata laluan pada komputer riba, telefon pintar, dan pemacu USB, dan jangan tinggalkan tanpa pengawasan.**

Item No 14 | Keselamatan pejabat

Jangan biarkan sesiapa menggunakan peranti tanpa kebenaran

Jangan tinggalkan komputer tanpa pengawasan. Komputer yang tidak diawasi boleh digunakan oleh sesiapa, contohnya, seseorang boleh log masuk tanpa kata laluan dan menggunakannya bagi tujuan yang tidak baik. Ambil langkah untuk melindungi komputer daripada penggunaan tanpa kebenaran.

Tindakan — **Ambil langkah, seperti *logout* daripada PC anda apabila meninggalkan meja, menutup PC apabila meninggalkan pejabat setiap hari, dan elakkan orang lain daripada menggunakan PC anda.**

Item No 15 | Keselamatan pejabat

Tegur jika orang tidak dikenali berada dalam kawasan premis syarikat

Kecurian maklumat boleh berlaku jika tidak mengehadkan akses untuk memasuki premis syarikat. Pastikan bahawa orang yang tidak berkenaan tidak dibenarkan mengakses tempat maklumat/dokumen penting disimpan, terutamanya seperti pelayan (server), arkib dan peti besi.

Tindakan — **Ambil langkah, seperti menghampiri dan menegur sesiapa yang anda tidak kenali di pejabat atau mewujudkan meja penyambut tetamu.**

Item No 16 | Keselamatan Pejabat

Ambil langkah untuk menghalang kecurian peralatan dan aksesori

Peranti seperti komputer riba, tablet, dan pemacu USB yang mudah alih menjadikannya berisiko tinggi untuk dicuri. Apabila peranti-peranti ini tidak digunakan, ambil langkah untuk menyimpannya di tempat yang selamat, seperti laci berkunci.

Tindakan — **Ambil langkah, seperti mengunci komputer riba, tablet, dan aksesori (CD, pemacu USB, pemacu keras luaran, dll.) dalam laci berkunci apabila meninggalkan pejabat.**

Item No 17 | Keselamatan Pejabat

Mengunci pintu pejabat

Menyimpan rekod orang terakhir meninggalkan pejabat juga membantu meningkatkan rasa bertanggungjawab bagi orang yang terakhir mengunci pintu.

Tindakan — **Ambil langkah, seperti menguruskan kunci dan menyimpan rekod orang terakhir meninggalkan pejabat dan mengunci pintu (tarikh, masa, dan nama).**

Item No 18 | Pelupusan maklumat dengan selamat

Lupuskan maklumat dengan cara yang betul

Sekadar membuang dokumen yang mengandungi maklumat penting ke dalam tong sampah boleh mengakibatkan kebocoran maklumat yang serius memandangkan orang lain boleh membaca dokumen itu. Tambahan lagi, maklumat yang disimpan di peranti elektronik dan media elektronik boleh didapatkan kembali walaupun jika fail telah dipadamkan. Apabila melupuskan maklumat penting, lupuskan setiap medium dengan betul, seperti menggunakan mesin perincih atau perisian pemadaman data.

Tindakan — **Ambil langkah untuk melupuskan maklumat, seperti menggunakan perisian pemadaman data, menghapuskannya secara fizikal, atau mendapatkan perkhidmatan pakar untuk memadamnya.**

Simpan dokumen yang mengandungi maklumat penting di dalam laci berkunci

Elakkan kecurian peranti

Kunci pintu pejabat

Bahagian 3 Pengurusan organisasi

Item No 19 hingga 25 adalah langkah-langkah yang perlu diambil setelah mewujudkan polisi untuk organisasi. Tingkatkan kesedaran pekerja dengan mendokumenkan dengan jelas peraturan keselamatan maklumat dan sebarkannya di pejabat.

Item No 19 Latihan pekerja

Pastikan pekerja memahami kewajipan mereka untuk mengekalkan kerahsiaan

Walaupun peraturan syarikat sudahpun memerlukan pekerja untuk mengekalkan kerahsiaan dalam kerja mereka, tetapi ia adalah bagus untuk memaklumkan pekerja mengenai peraturan syarikat dengan jelas untuk diikuti.

Tindakan Ambil langkah, seperti memaklumkan pekerja mengenai kewajipan mereka untuk mengekalkan kerahsiaan apabila mereka diambil bekerja.

Item No 20 Latihan pekerja

Jalankan latihan pekerja dengan kerap

Pekerja mengendalikan maklumat setiap hari dalam pelaksanaan kerja mereka, dan kebiasaan ini bermaksud terdapat kecenderungan untuk terlepas pandang dan lupa mengenai pengurusan maklumat dengan selamat. Latihan yang kerap adalah berkesan dalam meningkatkan kesedaran pekerja.

Tindakan Ambil langkah, seperti menerangkan kepentingan pengurusan maklumat dengan kerap dan menjalankan latihan dalaman.

Item No 21 Penggunaan peranti peribadi

Tentukan sama ada untuk membenarkan penggunaan peranti peribadi untuk tujuan kerja

Menjamin keselamatan menjadi sukar jika peranti peribadi seperti PC dan telefon pintar digunakan untuk tujuan kerja, kerana kesukaran untuk menguruskan penggunaannya oleh pekerja. Tentukan sama ada peranti peribadi boleh digunakan untuk tujuan kerja dan tetapkan peraturan penggunaannya.

Tindakan Ambil langkah, seperti mewujudkan sistem permohonan kebenaran untuk menggunakan peranti peribadi seperti PC dan telefon pintar untuk tujuan kerja dan tentukan peraturan penggunaannya jika ia dibenarkan.

Item No 22 Pematuhan kepada dasar/peraturan syarikat

Minta supaya rakan kongsi perniagaan mengekalkan kerahsiaan

Elakkan andaian bahawa rakan kongsi perniagaan akan mengekalkan kerahsiaan berdasarkan klasifikasi maklumat. Apabila memberikan maklumat sulit kepada rakan kongsi perniagaan, ia adalah penting untuk menyatakan bahawa ia perlu dianggap sebagai sulit.

Tindakan Ambil langkah, seperti merangka kontrak yang menyatakan kandungan maklumat yang perlu dianggap sebagai sulit.

Item No 23 Penggunaan perkhidmatan luaran

Gunakan perkhidmatan luaran yang boleh dipercayai

Jika anda mengutamakan kos dalam pemilihan perkhidmatan luaran seperti perkhidmatan awan, anda mungkin mendapati sesetengah perkhidmatan mungkin akan mengalami kegagalan atau masalah lain. Semak dengan teliti prestasi, kebolehpercayaan, butiran pampasan, dan pertimbangan lain yang berkenaan apabila menggunakan perkhidmatan luaran untuk aplikasi yang mempunyai kesan yang ketara atas kelangsungan perniagaan.

Tindakan Ambil langkah, seperti menyemak terma perkhidmatan, butiran pampasan, langkah-langkah keselamatan, dan perkara lain yang berkenaan apabila memilih vendor.

Penerangan dan Tindakan Disyorkan

Item No 24	Pengurusan Insiden

Bersedia menghadapi insiden keselamatan maklumat

Apabila insiden berlaku, kebiasaannya tidak ada masa untuk berfikir dengan tenang, dan sebarang kelewatan dalam tindak balas kepada insiden akan meningkatkan impak insiden itu. Gunakan insiden yang dilaporkan di media sebagai rujukan untuk berfikir mengenai siapa yang akan melakukan apa dan bila, mengandaikan bahawa perkara yang sama berlaku dalam syarikat anda.

Tindakan	Ambil langkah, seperti menyediakan manual tindak balas untuk kebocoran, kehilangan, atau kecurian maklumat penting.

Item No 25	Menyediakan peraturan

Wujudkan peraturan untuk langkah-langkah keselamatan maklumat

Walaupun dasar langkah-langkah keselamatan maklumat telah wujud, pekerja masih perlu merujuk kepada pengurus mereka melainkan jika dasar itu didokumenkan sebagai peraturan dalaman. Bagi membolehkan pekerja untuk bertindak mengikut undang-undang, dasar ini perlu didokumenkan dengan jelas sebagai “peraturan syarikat” supaya pekerja boleh merujuk kepadanya pada setiap masa.

Tindakan	Ambil langkah, seperti menjadikan item No. 1-24 dalam helaian penilaian ini sebagai peraturan untuk langkah-langkah keselamatan maklumat dan sebarkannya dalam syarikat serta semak semula peraturan-peraturan ini secara berkala untuk penambahbaikan apabila sebarang kekurangan ditemui.

NISC National center of Incident readiness and Strategy for Cybersecurity

NACSA AGENSI KESELAMATAN SIBER NEGARA NATIONAL CYBER SECURITY AGENCY

IPA Information-technology Promotion Agency, Japan

2019.04