|  |  |  |
| --- | --- | --- |
|  | **JABATAN PEMBANGUNAN KEMAHIRAN**  **KEMENTERIAN SUMBER MANUSIA**  **ARAS 7 & 8 BLOK D4, KOMPLEK D**  **PUSAT PENTADBIRAN KERAJAAN**  **PERSEKUTUAN**  **62530 PUTRAJAYA**    **KERTAS PENERANGAN**  (*INFORMATION SHEET*) | |
| **KOD DAN NAMA**  **PROGRAM /**  *PROGRAM’S CODE AND*  *NAME* | **Z-009-2:2015** **KEBOLEHAN TERAS** | |
| **TAHAP /** *LEVEL* | **2(DUA)** | |
| **NO. DAN TAJUK**  **KEBOLEHAN TERAS /**  *CORE ABILITY NO. AND*  *TITLE* | **CA01 APLIKASI KOMUNIKASI** | |
| **NO. DAN PENYATAAN**  **KEBOLEHAN /**  *ABILITY NO. AND*  *STATEMENT* | 01.01. GUNAKAN KOMUNIKASI 2 HALA  01.02. SEBARKAN MAKLUMAT SECARA ELEKTRONIK  01.03. SEBARKAN MAKLUMAT SECARA MANUAL  **01.03. TERAPKAN KERAHSIAAN MAKLUMAT** | |
| **NO. KOD /** *CODE NO.* | **Z-009-2:2015 M01/P(3/3)** | **Muka Surat** / *Page* : 1  **Drpd** / *of* : 12 |

**TAJUK***/TITLE* :  **KERAHSIAAN MAKLUMAT**

**TUJUAN***/PURPOSE* :

**Kertas Penerangan ini bertujuan untuk menerangkan mengenai** konsep, skop, prosedur dan kod kerahsiaan, tahap kejujuran dan integriti.

**PENERANGAN***/INFORMATION* :

1. **Konsep kerahsiaan**

Kerahsiaan boleh dianggap bersamaan dengan privasi. Langkah yang diambil untuk memastikan kerahsiaan direka untuk mencegah maklumat sensitif daripada sampai ke pihak yang tidak sepatutnya, di samping memastikan maklumat sampai kepada orang yang disasarkan: Akses mestilah terhad kepada orang-orang yang diberi kuasa sahaja.

* 1. Amalan biasa, data dikategorikan mengikut tahap dan jenis kerosakan yang boleh berlaku jika ia jatuh ke pihak yang tidak sepatutnya. Langkah-langkah pengukuhan kemudiannya boleh dilaksanakan mengikut kategori tersebut.

* 1. Melindungi kerahsiaan data mungkin melibatkan latihan khas bagi mereka yang mempunyai akses untuk dokumen-dokumen tersebut. Latihan tersebut biasanya akan merangkumi risiko keselamatan yang boleh mengancam maklumat. Latihan boleh membantu membiasakan mereka yang diberi akses dengan faktor-faktor risiko dan bagaimana untuk melindungi data tersebut.

* 1. Aspek latihan lanjutan adalah termasuk konsep kata laluan yang kukuh dan amalan terbaik pembinaan kata laluan dan maklumat yang berkaitan tentang konsep kejuruteraan sosial sebagai menghalang sebarang percubaan untuk melentur peraturan pengendalian data walaupun dengan niat yang baik tetapi mungkin memberikan hasil yang merosakkan.



Rajah 1. Simbol rahsia besar

* 1. Satu contoh kaedah baik yang digunakan untuk memastikan kerahsiaan apabila menggunakan perbankan dalam talian adalah nombor akaun atau nombor penghalaan ganti (*routing*). Enkripsi data ialah kaedah umum dalam memastikan kerahsiaan.

* 1. ID pengguna dan kata laluan merupakan satu prosedur standard; pengesahan dua faktor menjadi kebiasaan. Pilihan lain termasuk pengesahbetulan biometrik dan token keselamatan, kekunci fob atau token digital. Selain itu, pengguna boleh juga mengambil langkah-langkah untuk meminimumkan bilangan tempat maklumat itu diakses dan jumlah transaksi dilakukan.

Langkah-langkah tambahan mungkin akan diambil dalam kes dokumen yang sangat sensitif, langkah berjaga-jaga seperti menyimpan hanya pada komputer sekuriti siber, yang tidak bersambung ke peranti penyimpanan data, atau untuk maklumat yang sangat sensitif, dalam bentuk salinan cetak sahaja.

1. **Skop dan prosedur kerahsiaan**

Maklumat yang telah dikategorikan sebagai maklumat rahsia perlu dijaga dan dihormati hak privasi organisasinya. Maklumat kerahsiaan perlu difahami etikanya seperti:

* 1. Maklumat adalah Sulit

Maklumat perlu disimpan dengan selamat dan tidak mudah diakses. Maklumat yang sudah berada dalam domain awam secara amnya sukar dilindungi. Walau bagaimanapun, apabila berlakunya pelanggaran kepercayaan di pihak defendan yang menyebabkan maklumat tersebar kepada umum, defendan sendiri perlu bertanggungjawab terhadap kerugian dan kerosakan yang dialami oleh plaintif yang timbul daripada pendedahan tersebut.



Rajah 2 – Cap Sulit dan Rahsia di sampul surat

* 1. Dikemukakan dengan pengimportan kerahsiaan.

Maklumat ini telah disampaikan dalam keadaan yang membawa kepada kewajipan kerahsiaan. Penerima maklumat sulit hanya akan terikat jika penerima yang sepatutnya sedar bahawa maklumat yang disampaikan kepadanya adalah atas dasar keyakinan. Contoh yang paling jelas adalah apabila seseorang memberi maklumat dengan syarat ianya dirahsiakan. Walau bagaimanapun, mungkin timbul tanggungjawab kerahsiaan bergantung pada keadaan. Salah satu daripada contoh hubungan tanggungjawab kerahsiaan yang akan timbul ialah hubungan antara majikan dengan pekerja. Secara umumnya, dalam tempoh perkhidmatan pekerja mesti mematuhi suatu "kewajipan kesetiaan" terhadap majikannya serta bertindak demi kepentingan majikan.



Rajah 3. Suasana bekerja.

Ini termasuk melindungi rahsia perdagangan apabila pekerja itu terdedah ketika menjalankan tugas masing-masing. Sebaik sahaja pekerja tamat perkhidmatannya, dia masih bertanggungjawab untuk menjaga rahsia perdagangan bekas majikannya. Oleh itu, majikan berhak untuk menghalang bekas pekerja daripada menggunakan senarai pelanggan yang diketahui ketika masih berkhidmat dahulu dengan niat atau sengaja. Klausa perlindungan seperti itu bagaimanapun tidak meliputi kemahiran dan pengetahuan yang diperoleh pekerja berkhidmat dengan majikannya dahulu.

* 1. Berlaku pendedahan maklumat atau penggunaan tanpa kebenaran

Jika berlaku penggunaan atau pendedahan maklumat tanpa kebenaran yang telah dijangkakan. Tiada tindakan boleh dikenakan jika tiada berlaku pecah amanah dan tiada berlaku pendedahan yang tidak dibenarkan.

Apabila pendedahan atau penggunaan tanpa kebenaran dijangkakan, mahkamah akan dalam keadaan yang sesuai memberikan injunksi interlokutori untuk menghalang penggunaan atau pendedahan tanpa kebenaran. Mahkamah juga boleh mengarahkan ganti rugi bagi apa-apa kerugian atau kerosakan yang dialami akibat daripada pecah amanah, atau dalam keadaan tertentu, kerugian masa depan sebagai ganti injunksi.

* 1. Melindungi maklumat sulit

Tidak ada sistem pendaftaran untuk maklumat sulit. Perlindungan hanyalah dengan merahsiakan maklumat tersebut. Apabila ia terdedah kepada umum, maklumat berkenaan tidak boleh lagi dirahsiakan. Walaupun pemilik maklumat rahsia itu mahu mengambil tindakan undang-undang dan meminta pampasan atas kerosakan yang dialami, ia tidak mungkin sebaik seperti merahsiakan maklumat tersebut dari awalawal lagi. Aspek penting dalam mengekalkan perlindungan ialah pengurusan kawalan perniagaan yang secukupnya. Akses kepada maklumat sulit oleh kakitangan harus dihadkan oleh pihak pengurusan atas dasar "perlu tahu" sahaja, kerana punca utama kehilangan maklumat sulit sesebuah syarikat adalah apabila kakitangan berpindah ke syarikat lain dalam bidang kerja yang sama. Fasal yang sesuai perlu dimasukkan dalam kontrak pekerjaan dan kontrak dengan pihak ketiga seperti pembekal, subkontraktor dan sebagainya.

* 1. Perjanjian Tiada Pendedahan (NDA)

Perjanjian ini selalunya berlaku dalam perniagaan sesebuah syarikat yang perlu mendedahkan maklumat sulitnya kepada syarikat yang lain. Sebagai contoh, pengeluar mungkin perlu menghantar produk baharunya ke makmal ujian untuk penilaian teknikal dan kelulusan sebelum produk dilancarkan di pasaran. Kebiasaannya memang ada keperluan untuk berkongsi rahsia apabila dua buah syarikat mempertimbangkan untuk mengadakan beberapa bentuk kerjasama.

Dalam keadaan ini, memang dinasihatkan agar Perjanjian Tiada Pendedahan (NDA) digubal dan ditandatangani oleh pihak-pihak yang bersetuju untuk berkongsi tanggungjawab atas apa-apa maklumat sulit yang perlu dikongsi bersama. NDA memberikan perlindungan sekiranya tindakan undang-undang perlu diambil disebabkan pecah amanah, maka perkara itu boleh diuruskan seperti penguatkuasaan mana-mana kontrak perniagaan lain.



Rajah 4 . Makmal ujian.

* 1. Perlindungan Perjanjian Tidak Dedah Maklumat Di Bawah Fasal Antarabangsa 39 Perjanjian TRIPS (Perdagangan Berkaitan Aspek Hak Harta Intelek), yang mengikat negara anggota Pertubuhan Perdagangan Dunia, memerlukan perlindungan nilai komersial dan data tertentu maklumat tidak dedah dikemukakan kepada kerajaan atau agensi-agensi kerajaan, demi memastikan perlindungan yang berkesan terhadap persaingan yang tidak adil.

1. **Kejujuran dan integriti**

Kerahsiaan, integriti dan ketersediaan, adalah model yang direka untuk memberi panduan mengenai dasar demi keselamatan maklumat dalam sesebuah organisasi. Model ini juga kadang-kadang dirujuk sebagai AIC (ketersediaan, integriti dan kerahsiaan data).Unsur-unsur AIC adalah dianggap tiga komponen keselamatan yang paling penting.

Kejujuran dan keikhlasan adalah perlu dalam diri pekerja untuk mengekalkan maklumat kerahsiaan sesebuah organisasi. Dalam konteks ini, kerahsiaan ialah satu set peraturan yang mengehadkan akses kepada maklumat, integriti ialah jaminan bahawa maklumat boleh dipercayai dan tepat, dan ketersediaan ialah jaminan akses yang boleh dipercayai kepada maklumat oleh orang yang diberi kuasa.

* 1. Kerahsiaan

Kerahsiaan boleh dianggap bersamaan dengan privasi. Langkah yang diambil untuk memastikan kerahsiaan direka untuk mencegah maklumat sensitif daripada sampai kepada orang yang tak berkenaan, di samping memastikan bahawa yang berkenaan sahaja boleh mendapatkannya: Akses mesti terhad kepada mereka yang diberi kuasa untuk melihat data berkenaan. Adalah perkara biasa bagi data dikategorikan mengikut tahap dan jenis kerosakan yang boleh dilakukan jika ia jatuh ke tangan pihak yang tidak diingini. Kawalan ketat boleh dilaksanakan mengikut kategori berkenaan. Kadang-kadang demi melindungi kerahsiaan data mungkin melibatkan latihan khas bagi mereka yang ada akses khas untuk dokumen-dokumen berkenaan.

Latihan tersebut biasanya termasuk risiko keselamatan yang boleh mengancam maklumat berkenaan. Latihan boleh membantu mereka yang diberi kuasa membiasakan diri dengan faktor-faktor risiko dan bagaimana untuk mencegah risiko berkenaan.



Rajah 5. Data mesti dikriptografi.

* 1. Integriti

Integriti melibatkan mengekalkan ketekalan, ketepatan, dan kebolehpercayaan data melalui keseluruhan kitaran hidup data. Data tidak boleh berubah dalam transit, dan langkah-langkah perlu diambil untuk memastikan bahawa data tidak boleh diubah oleh orang yang tidak diberi kuasa (sebagai contoh, dalam pelanggaran kerahsiaan).

Langkah-langkah ini termasuk kebenaran fail dan kawalan capaian pengguna. Versi kawalan berbeza mungkin digunakan untuk mencegah masalah salah pindaan pemadaman tidak sengaja oleh pengguna yang diberi kuasa.

Di samping itu, beberapa cara perlu dilaksanakan untuk mengesan sebarang perubahan dalam data yang mungkin berlaku akibat daripada aktiviti yang bukan disebabkan oleh manusia seperti *electromagnet pulse* (EMP) atau kerosakan pelayan. Beberapa data mungkin perlu ada semakan semula atau semak kriptografi, untuk pengesahan integriti. Salinan data perlu disediakan untuk memulihkan data yang terjejas kepada keadaan yang betul jika berlaku kerosakan data.

* 1. Ketersediaan:

Cara terbaik memastikan ketersediaan adalah melalui penyelenggaraan semua perkakasan dengan rapi, melaksanakan pembaikan perkakasan serta-merta apabila diperlukan dan mengekalkan persekitaran sistem operasi yang berfungsi bebas daripada konflik perisian. Ia juga penting untuk memastikan peningkatan sistem yang diperlukan adalah yang terkini

Menyediakan komunikasi jalur lebar yang mencukupi dan mencegah berlakunya kejejalan komunikasi juga penting. Pengulangan, kegagalan, RAID dan gugusan ketersediaan yang tinggi boleh mengurangkan kesan yang serius apabila berlaku isu-isu perkakasan.

Tindakan pantas dan pemulihan bencana adalah penting jika berlaku senario kes terburuk; keupayaan tindakan itu bergantung pada kewujudan rancangan pemulihan bencana menyeluruh (DRP). Perlindungan terhadap kehilangan data atau gangguan dalam sambungan mesti mengambil kira kejadian tidak terduga seperti bencana alam dan kebakaran.

Untuk mengelakkan kehilangan data dari kejadian tidak terduga, satu salinan sokongan boleh disimpan di lokasi terpencil, selamat, bahkan dalam peti kalis api dan kalis air. Peralatan keselamatan tambahan atau perisian seperti *firewall* dan pelayan proksi boleh mengawal daripada kehilangan data ketika masa terhenti dan data tidak dapat dicapai disebabkan oleh tindakan yang berniat jahat seperti serangan penafian perkhidmatan (DoS) dan penerobosan rangkaian.

1. **Kod kerahsiaan**

Pekerja hendaklah melindungi maklumat yang diamanahkan kepada mereka dan tidak menyalahgunakan atau mendedahkannya secara salah. Kewajipan etika kerahsiaan mesti sentiasa seimbang terhadap pertimbangan etika persaingan atau undang-undang atau keperluan profesional yang memerlukan pendedahan maklumat yang diperoleh atau dicipta dalam konteks penyelidikan.

Sebagai contoh, dalam keadaan yang luar biasa dan terpaksa, pekerja atau penyelidik mungkin tertakluk kepada kewajipan untuk melaporkan maklumat kepada pihak berkuasa untuk melindungi kesihatan, nyawa atau keselamatan seseorang individu atau pihak ketiga. Penyelidik dikehendaki mengetahui kod etika (seperti kod tatakelakuan profesional) atau undang-undang (contohnya, mereka yang hendak melaporkan kanak-kanak yang memerlukan perlindungan) mungkin memerlukan pendedahan maklumat yang mereka peroleh dalam konteks penyelidikan. Dalam situasi lain pula, pihak ketiga mungkin akan cuba mendapatkan akses kepada maklumat yang diperoleh dan / atau diwujudkan keyakinan dalam konteks penyelidikan.

* 1. Penyelidik hendaklah juga memaklumkan kepada peserta dan dapatkan persetujuan mereka jika maklumat peribadi mereka mungkin akan dikongsi bersama dengan jabatan-jabatan kerajaan atau agensi, rakan-rakan komuniti dalam penyelidikan, anggota dari agensi yang memantau penyelidikan, penaja penyelidikan (seperti syarikat farmaseutikal), REB atau agensi kawal selia.



Rajah 6. Penyelidik di makmal.

Bagaimanapun, penyelidik boleh menyediakan data agregat yang tidak boleh dikaitkan dengan individu-individu kepada badan-badan pentadbiran untuk tujuan membuat dasar atau penilaian program. Apabila meminta keizinan, penyelidik hendaklah berbincang dengan peserta jika data terkumpul daripada projek boleh didedahkan, terutamanya jika pendedahan itu boleh menimbulkan risiko kepada peserta.

Sebagai contoh, data yang diberikan kepada pihak berkuasa mengenai penyelidikan mengenai penggunaan dadah haram dalam penjara yang boleh menimbulkan risiko tindakan balas kepada banduan, walaupun mereka tidak dikenal pasti secara individu.

* 1. Apabila merancang sesuatu kajian, penyelidik perlu mengaitkan mana-mana undang-undang berkaitan atau prinsip peraturan lain yang boleh memberi perlindungan terhadap privasi peserta dan kerahsiaan maklumat penyelidikan.

**SOALAN***/QUESTION* :

* + 1. Terangkan bagaimanakah caranya untuk memastikan maklumat kerahsiaan selamat?

....................................................................................................................................

....................................................................................................................................

* + 1. Mengapakah kod kerahsiaan diperlukan?

....................................................................................................................................

....................................................................................................................................