



PEJABAT SETIAUSAHA
KERAJAAN NEGERI SELANGOR

POLISI KESELAMATAN SIBER

— VERSI 1.0 —



RAKYAT



PERKHIDMATAN
DIGITAL



DATA & AWAN



INFRASTRUKTUR
KRITIKAL



AI & INOVASI



PERLINDUNGAN
DATA



TADBIR URUS



DAYA TAHAN &
KETERSEDIAAN



INTEGRITI ◆ KEBERDAYAAN ◆ KEPERCAYAAN ◆ KESELAMATAN

PKS PSUK SELANGOR 2026



PRAKATA

YB DATO' SETIAUSAHA KERAJAAN NEGERI SELANGOR

Assalamualaikum Warahmatullahi
Wabarakatuh dan Salam Sejahtera.

Alhamdulillah, setinggi-tinggi kesyukuran dirafakkan ke hadrat Allah SWT kerana dengan limpah kurnia dan izin-Nya, Polisi Keselamatan Siber Pejabat Setiausaha Kerajaan Negeri Selangor (PKS PSUK Selangor) berjaya direalisasikan. Penerbitan dokumen dasar ini menjadi panduan utama dan komitmen berterusan Kerajaan Negeri dalam menterjemahkan tadbir urus keselamatan siber yang utuh, sekali gus menjamin kelangsungan kerahsiaan, integriti, dan ketersediaan aset maklumat kerajaan agar sentiasa terpelihara pada tahap tertinggi.

Sejajar dengan kepesatan transformasi digital, PKS PSUK Selangor telah dirangka secara komprehensif berlandaskan peruntukan Akta Keselamatan Siber 2024 (Akta 854), pematuan piawaian antarabangsa ISO/IEC 27001:2022 serta amalan terbaik antarabangsa.



PRAKATA

Sejajar dengan kepesatan transformasi digital, PKS PSUK Selangor. Saya yakin pelaksanaan polisi ini adalah langkah strategik yang kritikal bagi memperkukuh kepercayaan rakyat terhadap keutuhan sistem penyampaian perkhidmatan digital kerajaan, di samping bertindak sebagai perisai utama dalam melindungi kepentingan dan data-data strategik Kerajaan Negeri Selangor.

Akhir kata, saya menyeru seluruh warga kerja Pejabat Setiausaha Kerajaan Negeri Selangor, Pejabat Daerah dan Tanah, jabatan, agensi, rakan strategik, pembekal serta semua pihak yang berkepentingan untuk bersama-sama menghayati dan mematuhi sepenuhnya ketetapan dalam PKS PSUK Selangor ini. Pembudayaan keselamatan siber menuntut kelangsungan kerjasama merentas agensi sebagai tanggungjawab kolektif. Semoga sinergi ini terus memacu aspirasi untuk menjadikan Selangor sebagai negeri yang berdaya tahan, berdaya saing, teguh dan makmur.

Sekian, terima kasih.

YB DATO' DR. AHMAD FADZLI BIN AHMAD TAJUDDIN
Setiausaha Kerajaan Negeri Selangor

MAKLUMAT DAN KAWALAN DOKUMEN

Polisi Keselamatan Siber Pejabat Setiausaha Kerajaan Negeri Selangor (PKS PSUK Selangor) merupakan dokumen dasar dan garis panduan yang menetapkan prinsip, keperluan serta kawalan keselamatan siber bagi melindungi aset digital, maklumat dan infrastruktur teknologi maklumat dan komunikasi milik Pejabat Setiausaha Kerajaan Negeri Selangor (PSUK) dan Pejabat Daerah dan Tanah (PDT) daripada ancaman, risiko dan insiden keselamatan siber. Polisi ini bertujuan memastikan kerahsiaan, integriti dan ketersediaan maklumat serta perkhidmatan ICT sentiasa terpelihara bagi menyokong penyampaian perkhidmatan kerajaan negeri yang selamat, berdaya tahan dan berkesinambungan.

Berasaskan Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO/IEC 27001:2022 dan Kod Tata Amalan Keselamatan Siber (*Code of Practice - COP*) PSUK Selangor, polisi ini menggariskan peraturan, kawalan dan prosedur standard yang wajib dipatuhi oleh semua pihak berkepentingan. Ini bagi memastikan rangkaian, sistem, data PSUK dan PDT Selangor sentiasa dilindungi daripada akses tanpa kebenaran, pelanggaran data serta serangan siber, sekali gus menjamin kerahsiaan, integriti dan ketersediaan maklumat awam.

PKS PSUK Selangor yang ditakrifkan merangkumi;

TARIKH	VERSI	KELULUSAN	TARIKH KUAT KUASA
30 Julai 2026	1.0	JPICT Bil. 4/2026	1 September 2026
		<>	

TAKRIFAN

TERMA	PENERANGAN
<i>Anti-malware</i>	Perisian yang mengimbas media storan seperti cakera optik, pita magnetik dan <i>flash disk</i> untuk sebarang kemungkinan perisian hasad.
<i>Application Programming Interface (API)</i>	Antara muka pengaturcaraan aplikasi ialah satu set peraturan dan protokol yang membenarkan aplikasi perisian yang berbeza untuk berkomunikasi dan berkongsi data antara satu sama lain.
<i>Artificial Intelligence (AI)</i>	Kecerdasan buatan ialah teknologi yang membolehkan sistem komputer melaksanakan fungsi yang biasanya memerlukan kecerdasan manusia seperti pembelajaran, analisis, penjanaan kandungan, automasi dan membuat keputusan.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
BKP	Bahagian Khidmat Pengurusan PSUK Selangor.
BPM	Bahagian Pengurusan Maklumat PSUK Selangor.
BPSM	Bahagian Pengurusan Sumber Manusia PSUK Selangor.
<i>Bring Your Own Device (BYOD)</i>	Peralatan mudah alih persendirian seperti telefon pintar, <i>tablet</i> , komputer riba dan media storan yang digunakan untuk tujuan rasmi.
<i>Chief Digital Officer (CDO)</i>	Ketua Pegawai Digital ialah pegawai yang dilantik untuk menjadi peneraju inisiatif pendigitalan di PSUK Selangor melalui penggunaan data, analitis dan teknologi digital.

TERMA	PENERANGAN
<i>Chief Government Security Office (CGSO)</i>	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia, iaitu sebuah unit di bawah Jabatan Perdana Menteri, Malaysia.
<i>Clear Desk dan Clear Screen</i>	Tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada di atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.
<i>Content Filtering</i>	Satu teknik yang menyekat atau membenarkan berdasarkan analisis kandungan dan bukannya berdasarkan sumber atau kriteria. Ia digunakan secara meluas untuk capaian internet dan email.
<i>Computer Security Incident Response Team (CSIRT)</i>	Pasukan Tindak Balas Insiden Keselamatan Siber, iaitu pasukan yang ditubuhkan untuk membantu agensi menguruskan pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
<i>Disaster Recovery Plan (DRP)</i>	Pelan Pemulihan Bencana atau DRP ialah satu dokumen rasmi yang mengandungi panduan langkah demi langkah tentang bagaimana sesebuah organisasi boleh memulihkan semula sistem IT, data dan operasi mereka dengan cepat selepas berlakunya sesuatu bencana. DRP merupakan bahagian penting dalam Pelan Pengurusan Kesenambungan Perkhidmatan.
E-mel	Maklumat atau mesej yang dihantar secara elektronik menerusi internet dari satu <i>endpoint</i> ke <i>endpoint</i> yang lain.
Enkripsi (<i>Encryption</i>)	Penukaran data sensitif kepada bentuk kod sulit untuk membolehkan data dikirim dengan selamat tanpa difahami pihak lain.
Entiti NCII	Entiti Infrastruktur Maklumat Kritikal Negara (<i>National Critical Information Infrastructure Entity-NCII</i>) ertinya mana-mana Entiti Kerajaan atau orang yang ditetapkan sebagai entiti infrastruktur maklumat kritikal negara di bawah seksyen 17 atau 18 (Rujuk Akta 854).

TERMA	PENERANGAN
<i>Generative AI</i>	Teknologi AI yang mampu menjana kandungan baharu seperti teks, imej, audio, video atau kod program berdasarkan arahan pengguna.
<i>Infrastructure as a service (IaaS)</i>	Merupakan model asas dalam pengkomputeran awan (<i>cloud computing</i>). IaaS menyediakan bahan binaan digital yang paling asas seperti komputer kosong (<i>virtual machines</i>), ruang storan dan rangkaian internet.
<i>Information and Communication Technology (ICT)</i>	Penggabungan teknologi maklumat dan teknologi komunikasi dalam perolehan, penyimpanan, pemprosesan dan pengagihan maklumat secara elektronik.
<i>ICT Security Officer (ICTSO)</i>	Pegawai Keselamatan ICT, iaitu pegawai yang dilantik untuk bertanggungjawab terhadap keselamatan siber.
Identiti (ID)	Identiti digital pengguna atau sistem. Berkaitan dengan: • <i>Identity Management</i> • <i>Authentication</i> • <i>Access Control</i>
<i>Intrusion Detection System (IDS)</i>	Sistem yang menyiasat semua aktiviti rangkaian dan mengenal pasti pola yang disyaki untuk menunjukkan bahawa rangkaian atau sistem dicerobohi.
Infrastruktur Maklumat Kritikal Negara (<i>National Critical Information Infrastructure, NCII</i>)	Infrastruktur Maklumat Kritikal Negara atau <i>NCII</i> ertinya suatu komputer atau sistem komputer yang gangguan pada atau kemusnahan komputer atau sistem komputer itu boleh membawa kesan yang memudaratkan terhadap penyampaian apa-apa perkhidmatan yang perlu bagi keselamatan, pertahanan, hubungan luar negara, ekonomi, kesihatan awam, kesejahteraan awam atau ketenteraman awam di Malaysia, atau terhadap keupayaan Kerajaan Persekutuan atau mana-mana Kerajaan Negeri untuk menjalankan fungsinya secara berkesan.

TERMA	PENERANGAN
Insiden Keselamatan Siber	Suatu perbuatan atau aktiviti yang dijalankan terhadap atau melalui suatu komputer atau sistem komputer, tanpa kuasa yang sah, yang membahayakan atau menjejaskan keselamatan siber komputer atau sistem komputer itu, atau komputer atau sistem komputer yang lain.
Internet	Sistem perangkaian antarabangsa yang membolehkan pengguna di seluruh dunia berhubung antara satu sama lain dan mencapai maklumat di seluruh dunia.
<i>Intellectual Property (IP)</i>	Hak pemilikan terhadap hasil ciptaan, idea, inovasi, karya, sistem atau produk yang dihasilkan oleh seseorang atau organisasi dan dilindungi oleh undang-undang.
<i>Intrusion Prevention System (IPS)</i>	Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan seperti <i>malicious code</i> .
<i>Information Security Management System (ISMS)</i>	Sistem Pengurusan Keselamatan Maklumat ISO/IEC 27001.
Jejak Audit (<i>Audit Trail</i>)	Log yang merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara.
JKPAK	Jawatankuasa Pengurusan Aset Alih Kerajaan
Kawasan Terperingkat	Meliputi kawasan premis atau sebahagian dari premis di mana rahsia rasmi disimpan atau diuruskan atau di mana kerja-kerja berkaitan rahsia rasmi dijalankan.
Kerentanan	Kelemahan atau kecacatan sistem atau aplikasi yang berisiko dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
Kriptografi	Penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak tertentu sahaja.

TERMA	PENERANGAN
<i>Local Area Network (LAN)</i>	Rangkaian komputer yang berkongsi data dan sumber dalam sesuatu kawasan yang terhad seperti sebuah bangunan dan sebuah pejabat.
<i>Large Language Model (LLM)</i>	Model AI berskala besar yang dilatih menggunakan data teks untuk memahami dan menjana bahasa manusia.
Media Storan	Peralatan elektronik yang digunakan untuk menyimpan data serta maklumat seperti cakera optik, pita magnetik, <i>flash disk</i> dan lain-lain media storan.
<i>National Cyber Security Agency (NACSA)</i>	Agensi Keselamatan Siber Negara (NACSA) ialah agensi peneraju keselamatan siber negara yang bertanggungjawab menyelaras dan memperkukuh tadbir urus, keupayaan serta ketahanan keselamatan siber Malaysia melalui penyelarasan kepakaran, sumber dan inisiatif keselamatan siber di peringkat nasional.
<i>Outsource</i>	Menggunakan perkhidmatan luar atau pihak ketiga untuk melaksanakan fungsi tertentu bagi suatu tempoh berdasarkan dokumen perjanjian dengan bayaran yang telah dipersetujui.
<i>Platform as a service(PaaS)</i>	Platform sebagai perkhidmatan atau <i>Platform as a service</i> . PaaS menyediakan satu platform atau persekitaran digital di atas talian (<i>cloud</i>) untuk pembangun (<i>developers</i>) membina, menguji, menjalankan dan menguruskan aplikasi atau perisian tanpa perlu memikirkan kos dan pengurusan infrastruktur asas.
Pegawai Aset Bahagian	Pegawai yang menyelaras dan memantau pengurusan aset di peringkat Bahagian.
Pegawai Aset ICT	Pegawai Aset ICT ialah pegawai dari BPM yang bertanggungjawab terhadap pengurusan aset ICT jabatan.
Pegawai Aset	Pegawai yang dilantik oleh Pegawai Pengawal/Pengerusi JKPAK untuk menyelaras dan memantau pengurusan aset jabatan termasuk aset alih dan stor (Unit Pengurusan Aset, BKP).

TERMA	PENERANGAN
Pegawai Aset Jabatan	Pegawai yang bertanggungjawab terhadap fasiliti, utiliti dan keselamatan fizikal – BKP (termasuk Unit Pentadbiran, Unit Pengurusan Aset serta Unit Keselamatan atau mana-mana pihak yang diberi tanggungjawab berkaitan) mengikut bidang kuasa yang ditetapkan.
Pembekal	Individu, entiti perkhidmatan atau organisasi yang menyediakan produk atau perkhidmatan kepada PSUK Selangor.
Pemilik Sistem	Pemilik perkhidmatan (<i>business owner</i>) bagi sistem yang dibangunkan atau bahagian atau unit di bawah PSUK Selangor yang paling banyak memiliki data dalam sesuatu sistem.
Pelan Kesyinambungan Perkhidmatan	Satu set prosedur yang membimbing entiti NCII untuk meneruskan operasi kritikal semasa dan selepas gangguan, seperti serangan siber atau bencana, dengan mengekalkan fungsi dan sistem penting serta membolehkan pemulihan cepat.
Pemilik Aset	Individu, jawatan atau unit yang dipertanggungjawabkan untuk mengurus, mengklasifikasikan, melindungi dan memastikan penggunaan sesuatu aset organisasi mengikut keperluan perniagaan, perundangan, peraturan serta dasar keselamatan maklumat yang berkuat kuasa.
Pemilik Maklumat	Pegawai atau pihak yang bertanggungjawab terhadap tadbir urus, pengelasan, penggunaan, perlindungan dan perkongsian maklumat, data digital, data awan dan data yang diproses menggunakan teknologi AI selaras dengan keperluan keselamatan maklumat, privasi, kedaulatan data dan peraturan yang berkuat kuasa.
Pengguna	Mana-mana individu, warga, pembekal, pihak ketiga atau entiti yang telah diberi kebenaran untuk mengakses, menggunakan atau mengurus sistem, aplikasi, data, rangkaian, perkhidmatan digital dan aset ICT PSUK dan PDT Selangor tertakluk kepada pematuhan PKS serta peraturan yang berkuat kuasa.

TERMA	PENERANGAN
Pentadbir Sistem ICT	Pegawai atau individu yang bertanggungjawab mengurus, memantau dan memastikan keselamatan sistem ICT, aplikasi, platform <i>cloud</i> , persekitaran virtual, sistem <i>Artificial Intelligence</i> (AI), rangkaian dan infrastruktur digital organisasi melalui pelaksanaan kawalan keselamatan, pengurusan akses dan pemantauan operasi secara berterusan.
Peralatan Mudah Alih	Peralatan mudah alih termasuk komputer riba dan peranti mudah alih seperti tablet, <i>Personal Digital Assistant</i> (PDA), telefon bimbit, telefon pintar, kamera digital dan sebagainya.
Perisian	Set atur cara komputer yang menjalankan tugas pada sistem komputer. Contoh perisian adalah sistem pengendali (Linux dan Windows), sistem utiliti (<i>Disk Cleanup</i> dan <i>Disk Defragmenter</i>), perisian aplikasi (<i>Microsoft Office</i> dan <i>Google Chrome</i>) dan lain-lain.
Perisian Hasad	Perisian hasad merupakan sebarang jenis perisian yang direka untuk membahayakan komputer seperti virus, <i>malware</i> , <i>ransomware</i> dan lain-lain.
Peralatan ICT	Peralatan ICT merujuk kepada semua aset fizikal teknologi maklumat dan komunikasi yang digunakan untuk memproses, menyimpan, menghantar, melindungi atau menyokong pengurusan maklumat dan penyampaian perkhidmatan organisasi. Contoh Peralatan ICT: komputer desktop, komputer riba, pelayan (<i>server</i>), pencetak pengimbas (<i>scanner</i>), peranti storan, suis rangkaian (<i>switch</i>), penghala (<i>router</i>), <i>firewall</i>, <i>access point</i> tanpa wayar.

TERMA	PENERANGAN
Peranti Titik Akhir (<i>Endpoint Device</i>)	<i>Endpoint Device</i> merujuk kepada peranti yang digunakan oleh pengguna untuk mengakses, memproses, menyimpan atau menghantar maklumat serta berhubung dengan sistem, aplikasi atau rangkaian organisasi. Contoh Peranti Titik Akhir: Komputer meja, komputer riba, <i>tablet</i>, telefon pintar, <i>thin client</i>, <i>virtual desktop</i> atau <i>virtual workstation</i>
Pihak Berkepentingan	Pihak berkepentingan ialah individu atau organisasi yang terlibat secara langsung atau tidak langsung, serta mempunyai kepentingan terhadap pengurusan, perlindungan dan pematuhan keselamatan maklumat dan keselamatan siber PSUK dan PDT Selangor.
Pihak Ketiga	Pakar runding, kontraktor dan individu yang mempunyai urusan dengan perkhidmatan ICT dan siber serta dilantik untuk melaksanakan tugas di PSUK dan PDT Selangor dalam jangka masa yang tertentu.
<i>Personal Identifiable Information</i> (PII)	Maklumat yang boleh digunakan secara tersendiri atau digunakan dengan maklumat lain untuk mengenal pasti individu tertentu.
<i>Public Key Infrastructure</i> (PKI)	Infrastruktur Kunci Awam, iaitu sistem enkripsi lengkap khusus untuk mencipta dan mengurus kekunci awam semasa proses penyulitan data dan pertukaran kekunci dalam kalangan pengguna. Ia merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
PKP	Pengurusan Kesenambungan Perkhidmatan (<i>Business Continuity Management</i>), bertujuan untuk memastikan fungsi-fungsi kritikal, perkhidmatan, sistem dan proses-proses utama dapat segera dipulihkan dalam masa yang ditetapkan sekiranya berlaku gangguan atau bencana.

TERMA	PENERANGAN
PKS PSUK Selangor	Polisi Keselamatan Siber PSUK Selangor, iaitu dokumen yang mengandungi dasar dan peraturan dalam menggunakan aset ICT di ruang siber.
PSUK Selangor	Pejabat Setiausaha Kerajaan Negeri Selangor.
PSUK dan PDT Selangor	Pejabat Setiausaha Kerajaan & Pejabat Daerah dan Tanah Negeri Selangor.
Rahsia Rasmi	Rahsia rasmi ertinya apa-apa surat yang dinyatakan dalam Jadual kepada Akta 88 dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit”, atau “Terhad”, mengikut mana-mana yang berkenaan, oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu Negeri atau Premier Sarawak atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta 88.
<i>Restore</i>	Aktiviti pemulihan atau penyalinan semula data daripada media penduaan.
<i>Router</i>	Peranti yang digunakan untuk menghantar data antara dua (2) rangkaian yang mempunyai kedudukan rangkaian yang berlainan.
Ruang siber	Ruang siber ialah suatu domain maya yang merangkumi keseluruhan ekosistem teknologi maklumat dan komunikasi, termasuk rangkaian, sistem komputer, aplikasi, data, infrastruktur digital dan komunikasi elektronik yang digunakan bagi tujuan operasi, penyampaian perkhidmatan, pengurusan maklumat dan transaksi digital.
Sandaran (<i>Backup</i>)	Proses penduaan sesuatu dokumen atau maklumat. Sumber yang boleh digunakan untuk menggantikan sumber utama yang gagal atau terhapus.
<i>Server</i>	Unit dalam rangkaian yang membekalkan data dan maklumat kepada komputer lain yang mempunyai hubungan rangkaian dengannya.

TERMA	PENERANGAN
Siber	Siber merujuk kepada persekitaran digital yang melibatkan penggunaan sistem komputer, rangkaian komunikasi, aplikasi, data dan teknologi maklumat yang saling berhubungan serta digunakan bagi menyokong operasi organisasi, penyampaian perkhidmatan dan pengurusan maklumat secara elektronik.
Sistem ICT	Merangkumi sistem aplikasi, sistem pusat data, rangkaian dan komunikasi ICT.
<i>Service Level Agreement (SLA)</i>	Perjanjian Tahap Perkhidmatan - Dokumen atau perjanjian rasmi yang menetapkan tahap perkhidmatan yang perlu disediakan oleh penyedia perkhidmatan kepada pengguna atau pelanggan dalam tempoh dan standard yang dipersetujui.
<i>Security Posture Assessment (SPA)</i>	Penilaian tahap kesiapsiagaan dan kedudukan keselamatan ICT sesebuah organisasi.
<i>Switch</i>	Peranti rangkaian yang digunakan untuk menghubungkan pelbagai peranti dalam sesuatu rangkaian komputer dan mengawal penghantaran data antara peranti berdasarkan alamat rangkaian bagi memastikan komunikasi data berlaku secara cekap dan selamat.
<i>Vulnerability Assessment and Penetration Testing (VAPT)</i>	Aktiviti teknikal untuk mengenal pasti dan menguji kelemahan keselamatan sistem.
Warga	Warga PSUK dan PDT Selangor termasuk pegawai yang berkhidmat secara kontrak atau pegawai khidmat singkat atau individu yang menjalankan praktikal di PSUK dan PDT Selangor yang menggunakan aset ICT dan siber secara langsung atau tidak langsung.
<i>Web Application Security Assessment (WASA)</i>	Penilaian keselamatan khusus untuk aplikasi web organisasi.
<i>Wide Area Network (WAN)</i>	Rangkaian komunikasi yang merangkumi kawasan geografi yang luas di seluruh bandar, negara atau rantau.

ISI KANDUNGAN

1	PENGENALAN	1
1.1	TUJUAN	3
1.2	OBJEKTIF	3
1.3	PERNYATAAN POLISI	4
1.4	PRINSIP KESELAMATAN	6
1.5	SKOP	11
1.6	TANGGUNGJAWAB DAN PENYELENGGARAAN	15
1.7	STRUKTUR	15
1.8	PEMAKAIAN	18
1.9	PENGECUALIAN POLISI	19
1.10	PENGUATKUASAAN	19
1.11	RUJUKAN	19

PERNYATAAN POLISI

SEKSYEN 1	: POLISI DAN OBJEKTIF KESELAMATAN SIBER	21
SEKSYEN 2	: TATA KELOLA	26
SEKSYEN 3	: KESELAMATAN SUMBER MANUSIA	49
SEKSYEN 4	: PENGURUSAN PEMBEKAL	55
SEKSYEN 5	: PENGURUSAN ASET	62
SEKSYEN 6	: PENGURUSAN RISIKO KESELAMATAN MAKLUMAT	73
SEKSYEN 7	: PERLINDUNGAN MAKLUMAT	80
SEKSYEN 8	: PENGURUSAN KESELAMATAN FIZIKAL	94
SEKSYEN 9	: PENGURUSAN KESELAMATAN RANGKAIAN	105
SEKSYEN 10	: PENGURUSAN KESELAMATAN SISTEM DAN APLIKASI	112
SEKSYEN 11	: PENGURUSAN IDENTITI DAN AKSES	126
SEKSYEN 12	: PENGURUSAN ANCAMAN DAN KERENTANAN	134
SEKSYEN 13	: PENGURUSAN PERISTIWA KESELAMATAN SIBER	137
SEKSYEN 14	: PENGURUSAN KESINAMBUNGAN	148
SEKSYEN 15	: UNDANG-UNDANG DAN PEMATUHAN	155
SEKSYEN 16	: DOKUMEN STANDARD PROSEDUR OPERASI	160
LAMPIRAN	: SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER	163
	PEJABAT SETIAUSAHA KERAJAAN NEGERI SELANGOR	
PENGHARGAAN :		166

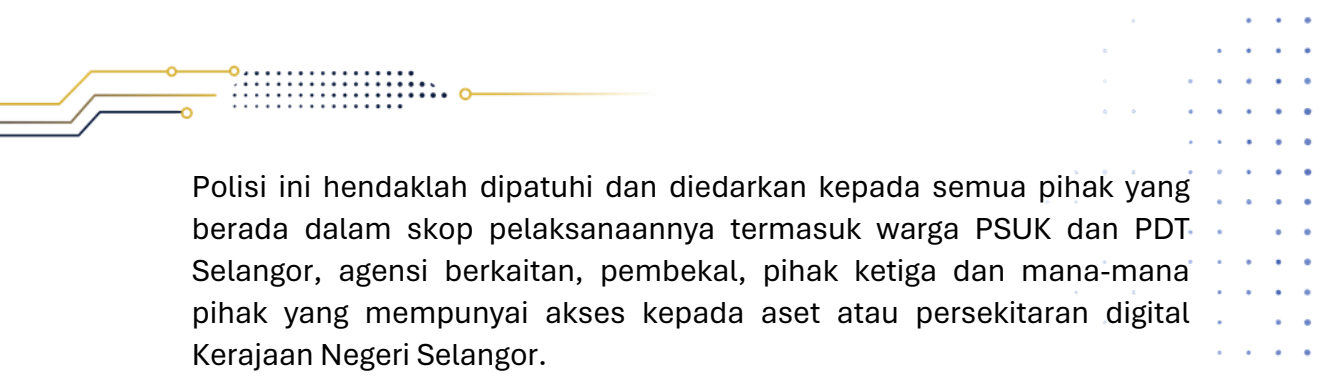
1. PENGENALAN

Pejabat Setiausaha Kerajaan Negeri Selangor (PSUK Selangor) telah mewujudkan Polisi Keselamatan Siber (PKS) sebagai langkah strategik bagi melindungi kerahsiaan, integriti dan ketersediaan aset maklumat serta memastikan keselamatan sistem maklumat yang digunakan untuk menyimpan, memproses dan menghantar maklumat rasmi Perkhidmatan Kerajaan Negeri Selangor.

Dalam era pendigitalan masa kini, pengurusan dan penyampaian perkhidmatan kerajaan amat bergantung kepada penggunaan Teknologi Maklumat dan Komunikasi (ICT). Maklumat merupakan aset strategik yang mempunyai nilai tinggi kepada PSUK dan PDT Selangor dan perlu dilindungi daripada sebarang risiko keselamatan, termasuk ancaman, kelemahan, penyalahgunaan, kehilangan, kebocoran atau kerosakan yang boleh menjejaskan kesinambungan perkhidmatan kerajaan.

Sehubungan itu, perlindungan keselamatan maklumat hendaklah dilaksanakan secara menyeluruh merangkumi keseluruhan kitaran hayat maklumat, termasuk proses penciptaan, penerimaan, pemprosesan, penyimpanan, penghantaran, perkongsian, perlindungan, arkib dan pemusnahan maklumat.

Pelaksanaan keselamatan maklumat yang berkesan melalui pendekatan mentakrif, melaksanakan, mengekalkan serta menambah baik kawalan keselamatan secara berterusan adalah penting bagi memastikan PSUK dan PDT Selangor dapat mencapai objektif organisasi, mengekalkan kepercayaan pemegang taruh, meningkatkan tahap pematuhan terhadap keperluan perundangan serta memperkukuh imej dan reputasi Kerajaan Negeri Selangor. Dokumen PKS ini merangkumi aspek keselamatan maklumat secara menyeluruh meliputi elemen tadbir urus organisasi, sumber manusia, keselamatan fizikal, keselamatan operasi dan perlindungan teknologi.



Polisi ini hendaklah dipatuhi dan diedarkan kepada semua pihak yang berada dalam skop pelaksanaannya termasuk warga PSUK dan PDT Selangor, agensi berkaitan, pembekal, pihak ketiga dan mana-mana pihak yang mempunyai akses kepada aset atau persekitaran digital Kerajaan Negeri Selangor.

PKS yang sentiasa dikemas kini dan relevan akan memastikan Kerajaan Negeri Selangor sentiasa bersedia mendepani landskap ancaman siber yang semakin kompleks dan dinamik melalui pelaksanaan dasar keselamatan siber yang holistik, proaktif dan inklusif. Pelaksanaan polisi ini juga bertujuan memperkukuhkan tahap daya tahan siber (*cyber resilience*) PSUK Selangor dalam memastikan semua aset maklumat, sistem digital dan infrastruktur maklumat kritikal negeri, khususnya yang dikategorikan sebagai *National Critical Information Infrastructure* (NCII), sentiasa dilindungi serta mampu bertahan, bertindak balas dan pulih dengan berkesan daripada sebarang serangan atau insiden keselamatan siber.

Polisi yang digariskan dalam dokumen ini menetapkan strategi keselamatan berdasarkan pengenalpastian domain pendekatan keselamatan, pengurusan risiko, pelaksanaan kawalan keselamatan yang sesuai, serta penetapan tanggungjawab yang jelas. Pelaksanaannya selaras dengan keperluan dasar, akta, arahan, peraturan, pekeliling, garis panduan kerajaan yang sedang berkuat kuasa serta amalan terbaik keselamatan siber yang berkaitan dan terpakai kepada persekitaran digital PSUK dan PDT Selangor dalam ruang siber.

Semua warga, pembekal, pihak ketiga serta pihak yang mempunyai urusan dengan perkhidmatan ICT PSUK dan PDT Selangor hendaklah membaca, memahami dan mematuhi kandungan PKS ini. Sebagai tanda aku janji pematuhan, semua pihak yang berkaitan hendaklah menandatangani borang pengakuan pematuhan PKS sebagai bukti bahawa mereka telah membaca, memahami dan bersetuju untuk mematuhi segala keperluan yang ditetapkan dalam polisi ini.

1.1 TUJUAN

Polisi Keselamatan Siber ini bertujuan untuk menerangkan, tanggungjawab, dasar, arahan, peraturan-peraturan, dan amalan yang MESTI DIBACA, DIFAHAMI dan DIPATUHI oleh warga PSUK dan PDT Selangor, pembekal, pihak ketiga dan pihak yang mempunyai urusan dengan perkhidmatan ICT dalam melindungi maklumat di ruang siber.

1.2 OBJEKTIF

PKS PSUK Selangor diwujudkan bagi memastikan infrastruktur maklumat kritikal dan juga semua aset maklumat dapat dilindungi daripada sebarang ancaman siber. Polisi ini merangkumi aspek keselamatan maklumat, keselamatan ICT dan juga keselamatan siber. Pelaksanaan PKS PSUK Selangor juga menyumbang kepada jaminan kesinambungan penyampaian perkhidmatan digital dan operasi yang bergantung kepada fungsi ICT di Kerajaan Negeri Selangor.

Objektif utama PKS ini adalah untuk:-

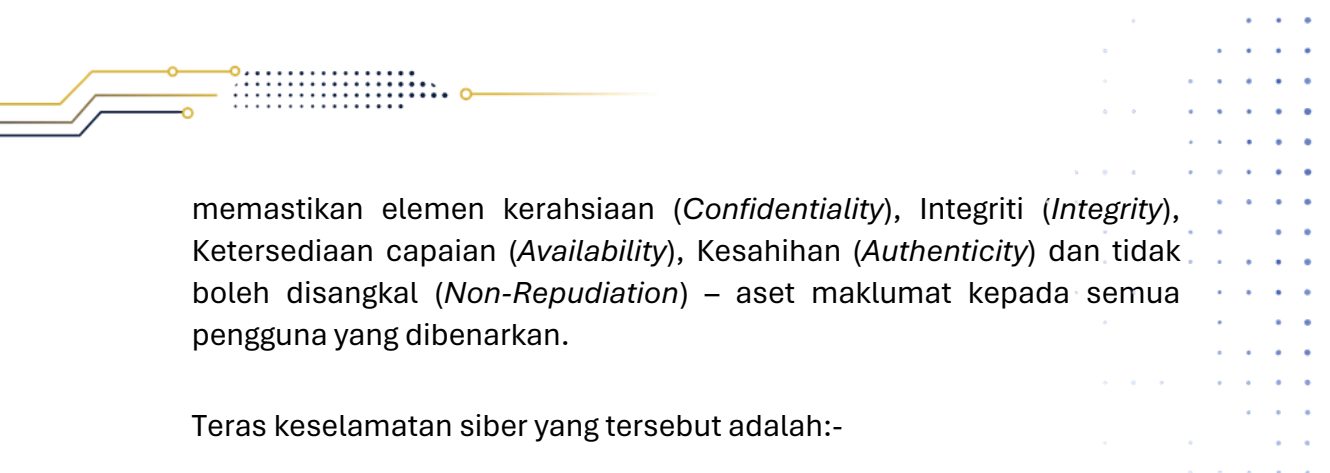
- i. Melindungi infrastruktur maklumat kritikal dan juga aset maklumat Kerajaan Negeri Selangor dari aspek Kerahsiaan, Integriti, Ketersediaan, Kesahihan dan Tidak Boleh Disangkal;
- ii. Memastikan keselamatan penyampaian perkhidmatan Kerajaan Negeri Selangor di tahap tertinggi menerusi pendekatan pengurusan risiko, pelaksanaan kawalan yang berkesan dan pemantauan keberkesanan kawalan keselamatan yang berterusan;
- iii. Menggariskan dasar berkaitan tugas dan tanggungjawab PSUK Selangor selaku peneraju sektor perkhidmatan bagi melindungi Infrastruktur Maklumat Kritikal Negara (NCII);

- 
- iv. Menetapkan dan tanggungjawab serta tadbir urus keselamatan siber;
 - v. Memastikan keperluan dan melindungi pihak berkepentingan seperti jabatan dan agensi kerajaan, pihak industri dan orang awam;
 - vi. Mengenal pasti dan menetapkan domain keselamatan siber yang berkaitan;
 - vii. Memastikan kelancaran operasi serta menjamin kesinambungan perkhidmatan digital ataupun mana-mana perkhidmatan yang bergantung kepada ICT;
 - viii. Memastikan perkongsian maklumat yang selamat;
 - ix. Mencegah salah guna atau kecurian maklumat;
 - x. Mengurangkan impak dan kesan akibat insiden keselamatan yang menyebabkan gangguan dari segi kerahsiaan, integriti, kebolehsediaan, kebocoran maklumat dan kegagalan infrastruktur maklumat;
 - xi. Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan siber; dan
 - xii. Memastikan pematuhan kepada keperluan tadbir urus dan perundangan yang berkaitan.

1.3 PERNYATAAN POLISI

Aset maklumat ialah aset kritikal yang bernilai kepada PSUK dan PDT Selangor mestilah dilindungi dengan sewajarnya. Keselamatan aset maklumat adalah suatu proses yang berterusan dan melibatkan aktiviti berkala yang mesti dilakukan dari masa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan siber sentiasa berubah.

Perlindungan aset maklumat ini merangkumi perlindungan semua bentuk maklumat dan data elektronik yang diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bagi memelihara keselamatan aset maklumat dalam ruang siber untuk



memastikan elemen kerahsiaan (*Confidentiality*), Integriti (*Integrity*), Ketersediaan capaian (*Availability*), Kesahihan (*Authenticity*) dan tidak boleh disangkal (*Non-Repudiation*) – aset maklumat kepada semua pengguna yang dibenarkan.

Teras keselamatan siber yang tersebut adalah:-

- i. Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.
- ii. Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini dan hanya boleh diubah dengan cara yang dibenarkan.
- iii. Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.
- iv. Kesahihan - Data dan maklumat hendaklah dipastikan kesahihannya.
- v. Tidak Boleh Disangkal - Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal.

Selain itu, langkah-langkah melindungi keselamatan aset maklumat hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan landskap keselamatan siber semasa, tahap kepentingan aset maklumat dan juga infrastruktur maklumat kritikal, ancaman dan kelemahan yang wujud, risiko yang mungkin timbul dan langkah-langkah pencegahan yang perlu diambil untuk menangani risiko berkenaan. Penetapan kawalan keselamatan yang sesuai hendaklah berdasarkan klasifikasi data dan maklumat atau nilai/kepentingan aset maklumat. Klasifikasi data dan maklumat ini boleh merujuk kepada arahan/pekeliling/garis panduan kerajaan yang berkuat kuasa.

Keselamatan aset maklumat adalah tanggungjawab warga, pembekal, pihak ketiga dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Selangor dalam melindungi aset maklumat.

1.4 PRINSIP KESELAMATAN

Prinsip-prinsip yang menjadi asas kepada PKS PSUK Selangor adalah seperti berikut:

i. **Akses Atas Dasar Perlu Mengetahui**

Akses terhadap penggunaan aset maklumat hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan.

ii. **Hak Akses Minimum**

Pengguna hendaklah diberikan hak akses minimum iaitu terhadap kepada keperluan untuk menjalankan tugasnya. Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujudkan, menyimpan, mengemas kini, mengubah atau membatalkan maklumat tertentu. Hak akses atau capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan tersebut. Hak akses perlu dikaji dari masa ke semasa berdasarkan kepada dan tanggungjawab pengguna/bidang tugas.

iii. **Akauntabiliti**

Semua pengguna bertanggungjawab ke atas semua tindakannya terhadap aset maklumat PSUK dan PDT Selangor.

Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber/aset maklumat. Untuk menentukan tanggungjawab ini dipatuhi, sistem/aplikasi ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem/aplikasi boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

- a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
- b) Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
- c) Menentukan maklumat sedia untuk digunakan;
- d) Menjaga kerahsiaan kata laluan;
- e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
- f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
- g) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.

iv. **Pengasingan Tugas**

Bagi mengekalkan prinsip sekat-dan-imbang (*check and balance*), Kerajaan Negeri Selangor hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya. Tugas mewujudkan, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset maklumat daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian, keselamatan dan aplikasi mengikut kesesuaian;

v. **Prinsip Kedalaman Pertahanan**
(*Defense in Depth*)

Prinsip ini adalah strategi pertahanan siber yang menggunakan pelbagai lapisan kawalan untuk melindungi aset maklumat dan infrastruktur maklumat kritikal. Konsepnya ialah jika satu lapisan pertahanan terjejas, lapisan selanjutnya boleh melindungi pada peringkat berikutnya. Pendekatan ini menggabungkan pelbagai langkah keselamatan untuk melindungi daripada ancaman dan meningkatkan daya tahan keseluruhan mekanisme pertahanan.

vi. **Prinsip Keselamatan menerusi Reka bentuk**
(*Security by Design*)

Prinsip ini ialah pendekatan untuk menyepadukan prinsip dan amalan keselamatan ke dalam reka bentuk dan pembangunan sistem, perisian dan rangkaian sejak awal. Matlamatnya adalah untuk menangani kelemahan keselamatan secara proaktif dan memastikan mekanisme perlindungan yang kukuh disediakan sebelum sistem digunakan.

vii. **Prinsip Kepercayaan Sifar**
(*Zero Trust*)

Prinsip ini meliputi konsep keselamatan yang bertujuan untuk meningkatkan postur keselamatan keseluruhan Kerajaan Negeri Selangor dengan menganggap setiap peranti dan pengguna, di dalam dan di luar perimeter rangkaian, berpotensi terjejas akibat gangguan insiden siber. Oleh demikian, tiada *endpoint* pengguna atau peranti boleh dipercayai secara automatik dan setiap permintaan untuk capaian rangkaian hendaklah disahkan seolah-olah berasal dari rangkaian terbuka.

Di bawah prinsip ini:-

- a. Semua trafik rangkaian (dalaman dan luaran) dianggap tidak dipercayai.
- b. Akses kepada sumber diberikan berdasarkan set kriteria yang komprehensif, termasuk identiti pengguna, kesihatan peranti, lokasi, dan faktor kontekstual lain yang berkaitan. Akses kepada sumber tanpa mengira lokasi hanya diberikan setelah pengesahan pengguna dan peranti berjaya.
- c. Menekankan prinsip keistimewaan yang paling sedikit, berikan akses kepada sumber yang perlu diakses, apabila diperlukan dan hanya untuk tempoh masa.

viii. **Pengauditan**

Pengauditan keselamatan siber ialah proses memeriksa dan menilai dasar dan amalan dan postur keselamatan siber organisasi secara sistematik untuk memastikan keberkesannya terhadap ancaman siber. Ini melibatkan penilaian kawalan teknikal dan pentadbiran sedia ada, mengenal pasti kelemahan dan potensi risiko, serta memastikan pematuhan terhadap piawaian dan peraturan keselamatan yang berkaitan. Aset maklumat seperti sistem, aplikasi, pangkalan data, komputer, pelayan, *router*, *firewall* dan peralatan rangkaian dan lain-lain hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*.

ix. **Daya Tahan Siber** (*Cyber Resilience*)

Pemulihan segera infrastruktur maklumat kritikal adalah penting, khususnya bagi sistem dan aplikasi yang dikategorikan sebagai misi kritikal seperti sistem yang menyokong kesiapsiagaan pertahanan siber dan sistem yang diperlukan untuk pengoperasian aset Kerajaan Negeri Selangor. Terdapat juga sistem kritikal seperti sistem yang menyokong fungsi kewangan



dan juga sistem berkaitan kesihatan. Semua aset maklumat dan infrastruktur maklumat kritikal mestilah mempunyai ketahanan siber (*Cyber Resilience*).

Daya tahan siber merujuk kepada keupayaan organisasi untuk membuat persediaan, bertindak balas dan pulih daripada serangan dan insiden siber. Ketahanan siber membolehkan organisasi menghadapi ancaman siber dan mengekalkan fungsi pentingnya dengan gangguan minimum. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada insiden keselamatan siber ataupun bencana yang menjejaskan fungsi aset maklumat dan juga infrastruktur maklumat kritikal. Pemulihan boleh dilakukan melalui pelbagai strategi seperti aktiviti penduaan data dan mewujudkan pelan pemulihan bencana, pelan kesinambungan perkhidmatan organisasi. Pada dasarnya, prinsip ini menggabungkan elemen keselamatan siber, kesinambungan perkhidmatan dan tindak balas insiden untuk mewujudkan pendekatan holistik untuk mengurus dan mengurangkan risiko siber.

x. **Saling Bergantungan**

Setiap prinsip di atas saling melengkapi dan saling bergantung. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan seperti *Defense in Depth* dan *Security by Design* adalah perlu bagi menjamin keselamatan yang maksimum.

xi. **Pematuhan**

Pematuhan adalah penting untuk mewujudkan persekitaran keselamatan siber yang terjamin, melindungi maklumat sensitif dan mengekalkan kepercayaan dan kredibiliti aset maklumat dan infrastruktur maklumat kritikal. Pematuhan kepada keperluan undang-undang, peraturan dan piawaian membantu organisasi



mengelakkan implikasi undang-undang dan sebarang penalti atau tindakan punitif daripada pihak Kerajaan dan pihak berkepentingan. PKS PSUK Selangor hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran yang boleh mewujudkan ruang ancaman keselamatan siber.

1.5 SKOP

Polisi dalam dokumen ini adalah meliputi semua infrastruktur maklumat kritikal dan juga aset maklumat yang berada di bawah tanggungjawab PSUK Selangor. Aset maklumat Kerajaan Negeri Selangor terdiri daripada data dan maklumat sama ada dalam bentuk salinan digital (*softcopy*) atau salinan bercetak (*hardcopy*), perkakasan (*hardware*), perisian (*software*), infrastruktur ICT, manusia (*people*) dan premis.

PKS menetapkan keperluan-keperluan asas seperti berikut:

- i. Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan yang tepat dibuat dan penyampaian perkhidmatan yang berkualiti dapat dilaksanakan.
- ii. Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Aset maklumat ini terjamin keselamatannya sepanjang masa, PKS ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur pengendalian semua perkara berikut:

i. **Data atau Maklumat**

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif PSUK Selangor. Contohnya sistem dokumentasi, prosedur operasi, rekod-rekod PSUK dan PDT Selangor, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

ii. **Salinan Digital**

(Softcopy)

Koleksi dokumen dalam digital atau elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif Selangor;

iii. **Salinan Bercetak**

(Hardcopy)

Koleksi dokumen dalam bentuk kertas atau bercetak, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif organisasi (contohnya: sistem dokumentasi, prosedur operasi, rekod-rekod, profil pelanggan, fail-fail dan lain-lain);

iv. **Perkakasan**

(Hardware)

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan PSUK dan PDT Selangor. Contoh peralatan dan periferal seperti komputer, pelayan, *firewall*, pencetak, peralatan media, peralatan komunikasi dan alat-alat prasarana seperti *Uninterruptible Power Supply* (UPS) dan sebagainya;

v. **Perisian**
(*Software*)

Program, prosedur, atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat; dan

vi. **Infrastruktur ICT**

Merujuk kepada set lengkap perkakasan, perisian, rangkaian, dan yang membolehkan penghantaran, penyimpanan, pemprosesan dan mendapatkan semula maklumat dalam organisasi atau merentasi pelbagai organisasi. Ini termasuklah sistem komputer, pelayan, pangkalan data, rangkaian, sambungan internet, sistem komunikasi, pusat data, perkhidmatan pengkomputeran awan (*cloud computing*) dan peralatan dan teknologi lain yang diperlukan. Infrastruktur ICT yang direka bentuk dan dilaksanakan untuk menyokong dan membolehkan pelbagai jenis perkhidmatan dan aplikasi teknologi maklumat dan komunikasi dalam Kerajaan Negeri Selangor berfungsi bagi mencapai objektif dan misi yang ditetapkan.

Infrastruktur ICT ini termasuk:

- a) Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
- b) Sistem Kawalan akses seperti sistem kad akses;
- c) Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain; dan
- d) Perkhidmatan sokongan seperti kemudahan elektrik, pendingin hawa, sistem pencegahan kebakaran, sistem pemantauan CCTV dan lain-lain.

vii. **Manusia**

Semua pengguna infrastruktur ICT PSUK dan PDT Selangor yang dibenarkan, termasuk kakitangan, pengguna dan pembekal. Individu yang mempunyai pengetahuan untuk melaksanakan skop kerja harian bagi mencapai misi dan objektif jabatan. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

viii. **Premis**

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (i) - (vii) di atas.

Setiap perkara di atas perlu diberi perlindungan yang rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan dianggap sebagai pelanggaran terhadap langkah-langkah keselamatan.

Sehubungan dengan itu, pematuhan terhadap PKS ini menjadi tanggungjawab semua warga. Setiap individu hendaklah memahami masing-masing dalam memastikan keselamatan maklumat sentiasa terpelihara, selaras dengan keperluan dasar, peraturan dan amalan terbaik yang ditetapkan.

Pelaksanaan PKS ini adalah berteraskan prinsip-prinsip berikut:

i. **TADBIR URUS**

(Governance):

Menetapkan dasar, prosedur serta mekanisme pengawasan yang jelas bagi memastikan strategi keselamatan maklumat sejajar dengan objektif perkhidmatan PSUK Selangor. Ia juga memastikan akauntabiliti diperkukuhkan dan pelaburan dalam keselamatan dioptimumkan bagi menyokong operasi perkhidmatan secara berkesan.

ii. **RISIKO**

(*Risk*):

Mengenal pasti, menilai dan mengurus risiko keselamatan maklumat secara sistematik bagi memastikan tahap risiko berada dalam had toleransi organisasi. Pendekatan ini membolehkan keputusan yang lebih berinformasi dan bersepadu dibuat, serta meningkatkan pihak kefahaman terhadap landskap risiko dalam kalangan berkepentingan.

iii. **PEMATUHAN**

(*Compliance*):

Memastikan semua aktiviti dan pengurusan keselamatan maklumat mematuhi keperluan perundangan, peraturan, kontrak serta garis panduan yang berkuat kuasa. Pematuhan ini penting bagi melindungi kepentingan organisasi serta mengekalkan kepercayaan pihak berkepentingan.

1.6 TANGGUNGJAWAB DAN PENYELENGGARAAN

Dokumen PKS dimiliki oleh PSUK Selangor yang bertanggungjawab untuk semakan dan penyelenggaraan dokumen sekurang-kurangnya sekali setahun dan/atau apabila berlaku perubahan ketara untuk memastikan organisasi sentiasa dikemas kini dengan peraturan dan teknologi terkini, serta konsisten dengan amalan terbaik industri; dan untuk mengagihkannya kepada warga dan pihak berkenaan.

1.7 STRUKTUR

Secara amnya, struktur polisi ini dibahagikan kepada 16 seksyen seperti berikut:

SEKSYEN 1 : Polisi dan Objektif Keselamatan Siber

Menetapkan hala tuju, prinsip dan objektif keselamatan siber bagi melindungi aset maklumat melalui dasar yang jelas, pelaksanaan berstruktur serta semakan berterusan untuk memastikan keberkesanan.

SEKSYEN 2 : Tata Kelola *(Governance)*

Menentukan tanggungjawab dan struktur tadbir urus keselamatan siber bagi memastikan pengurusan, pelaksanaan dan pemantauan keselamatan maklumat dilaksanakan secara menyeluruh dan berakauntabiliti.

SEKSYEN 3 : Keselamatan Sumber Manusia

Memastikan semua warga, pembekal dan pihak berkepentingan memahami serta mematuhi tanggungjawab keselamatan maklumat melalui tapisan, latihan, kesedaran dan tindakan disiplin.

SEKSYEN 4 : Pengurusan Pembekal

Memastikan risiko keselamatan maklumat yang berkaitan dengan pembekal, pihak ketiga dan rantai bekalan diurus secara berkesan bagi melindungi aset, sistem dan data PSUK dan PDT Selangor.

SEKSYEN 5 : Pengurusan Aset

Mengurus dan melindungi aset ICT serta maklumat melalui inventori, penggunaan terkawal, penyelenggaraan dan pelupusan yang selamat bagi mengelakkan kebocoran atau penyalahgunaan.

SEKSYEN 6 : Pengurusan Risiko Keselamatan Maklumat

Mengenal pasti, menilai, merawat dan memantau risiko keselamatan maklumat secara sistematik bagi memastikan risiko berada pada tahap yang boleh diterima.

SEKSYEN 7 : Perlindungan Maklumat

Melindungi maklumat melalui pengelasan, kawalan pemindahan, perlindungan rekod, pencegahan *malware* serta kawalan kebocoran data bagi menjamin kerahsiaan, integriti dan ketersediaan.

SEKSYEN 8 : Pengurusan Keselamatan Fizikal

Melindungi kemudahan fizikal, premis dan peralatan ICT daripada akses tanpa kebenaran, kerosakan dan ancaman persekitaran melalui kawalan keselamatan yang sesuai.

SEKSYEN 9 : Pengurusan Keselamatan Rangkaian

Memastikan rangkaian ICT dilindungi melalui kawalan akses, pemantauan, pengasingan rangkaian dan penapisan kandungan bagi mencegah ancaman siber.

SEKSYEN 10 : Pengurusan Keselamatan Sistem dan Aplikasi

Menjamin keselamatan sistem dan aplikasi melalui kawalan konfigurasi, pembangunan selamat, ujian keselamatan dan pengurusan perubahan sepanjang kitar hayat sistem.

SEKSYEN 11 : Pengurusan Identiti dan Akses

Mengawal akses kepada sistem dan maklumat melalui pengurusan identiti, pengesahan pengguna dan kawalan hak akses berdasarkan keperluan tugas.

SEKSYEN 12 : Pengurusan Ancaman dan Kerentanan

Mengenal pasti, menilai dan mengurus ancaman serta kerentanan teknikal secara proaktif bagi mengelakkan eksploitasi dan serangan siber.

SEKSYEN 13 : Pengurusan Peristiwa Keselamatan Siber

Mengurus insiden keselamatan secara sistematik melalui pengesanan, pelaporan, tindak balas, pembelajaran dan pengumpulan bukti untuk penambahbaikan berterusan.

SEKSYEN 14 : Pengurusan Kesenambungan

Memastikan kesinambungan operasi melalui pelan pemulihan bencana, sandaran data dan keupayaan pemulihan sistem semasa gangguan atau insiden.

SEKSYEN 15 : Undang-Undang dan Pematuhan

Memastikan pematuhan kepada keperluan perundangan, piawaian dan kontrak termasuk perlindungan data peribadi serta hak harta intelek.

SEKSYEN 16 : Dokumen Standard Prosedur Operasi (SOP)

Menetapkan keperluan dokumentasi prosedur operasi yang jelas, terkawal dan dikemas kini bagi memastikan operasi ICT dilaksanakan secara konsisten dan selamat.

1.8 PEMAKAIAN

Polisi Keselamatan Siber ini terpakai kepada semua warga, pembekal dan pihak ketiga serta mana-mana pihak yang mempunyai akses kepada sistem, data dan infrastruktur ICT organisasi tanpa pengecualian tanpa pengecualian.

1.9 PENGECUALIAN POLISI

Sebarang pengecualian PKS perlu disahkan oleh ICTSO dan diluluskan oleh CDO.

1.10 PENGUATKUASAAN

Semua warga, pembekal, pihak ketiga dan pihak berkepentingan tertakluk kepada pematuhan PKS ini. Sebarang pelanggaran atau ketidakpatuhan akan dikenakan tindakan tatatertib atau perundangan selaras dengan peraturan dan undang-undang yang berkuat kuasa.

1.11 RUJUKAN

Nama Dokumen	No Rujukan	Penerbit
Akta Keselamatan Siber 2024	CSA 854	Kerajaan Malaysia
Akta Rahsia Rasmi 1972	Akta 88	Kerajaan Malaysia
Dasar Keselamatan ICT	DKICT PSUK Selangor 4.0	Pejabat SUK Selangor
Tataamalan Bagi Entiti Infrastruktur Maklumat Kritikal Negara (<i>National Critical Information Infrastructure NCII</i>) Negeri Selangor	COP NCII	Pejabat SUK Selangor
<i>Information Technology Security Techniques-Information Security Management Systems Requirements (3rd Revision)</i>	ISO/IEC 27001:2022	<i>International Standard</i>
<i>Information Technology Security Techniques-Code of Practices for Information Security Controls (3rd Revision)</i>	ISO/IEC 27002:2022	<i>International Standard</i>
<i>Information technology- Security techniques- Privacy framework</i>	ISO/IEC 29100:2011	<i>International Standard</i>
Perolehan Perkhidmatan Pengkomputeran Awan (Cloud) Sektor Awam	PK 2.6 (2023)	Pekeliling Perbendaharaan, Kerajaan Malaysia

Nama Dokumen	No Rujukan	Penerbit
Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021	Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU) Jabatan Perdana Menteri
Dasar Perkongsian Data Selangor (DPDS)	Versi 1.0 Tahun 2023	Pejabat SUK Selangor
Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan dalam Perkhidmatan Awam.	Surat Pekeliling Am Bilangan 2 Tahun 2021 versi 2.0	Kerajaan Malaysia
Garis Panduan Pengurusan Dan Pengendalian Rahsia Rasmi Dalam Perkhidmatan Awam, 2024	Surat Pekeliling Am Bilangan 8 Tahun 2024	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO)
Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam	Pekeliling Am Bil. 4/2022	<i>National Cyber Security Agency (NACSA)</i>
Security and Privacy Controls for Information Systems and Organizations	NIST SP800-53	<i>National Institute of Standards and Technology, USA.</i>
Surat Pekeliling Am Bil. 1 Tahun 2020 – Pemakluman Pemakaian dan Penguatkuasaan Arahan Keselamatan (Semakan dan Pindaan 2017)	KPKK(R)100-1/5/4 Jld.2(15)	Ketua Pengarah Keselamatan Kerajaan (CGSO)
Akta Jenayah Komputer 1997	Akta 588	Kerajaan Malaysia
Akta Perwakilan Kuasa 1956	Akta 563	Kerajaan Malaysia
Akta Komunikasi dan Multimedia 1998	Akta 358	Kerajaan Malaysia
Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam	Surat Pekeliling Am Bil. 4/2024	Jabatan Perdana Menteri
Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT (PTK ICT)	Surat Pekeliling Am Bil. 4/2024	Jabatan Perdana Menteri



SEKSYEN 1

POLISI DAN OBJEKTIF KESELAMATAN SIBER

*Cyber Security Objective
and Policy*

POLISI DAN OBJEKTIF KESELAMATAN SIBER

CYBER SECURITY OBJECTIVE AND POLICY

PERNYATAAN POLISI

SEKSYEN 1 : POLISI DAN OBJEKTIF KESELAMATAN SIBER (Cyber Security Objective and Policy)

1.1 (A.5.1) Polisi Untuk Keselamatan Maklumat (Policies for Information Security)

Objektif: Untuk memastikan kesesuaian, kecukupan dan keberkesanan berterusan terhadap hala tuju pengurusan serta sokongan bagi keselamatan maklumat selaras dengan keperluan perkhidmatan, perundangan, statutori, kawal selia dan kontrak.

1.1.1 Pelaksanaan Polisi (Execution of the Policy)

Pernyataan

- i. Satu set polisi untuk keselamatan maklumat/siber perlu ditakrifkan, diluluskan, diterbitkan, dimaklumkan dan dipatuhi kepada warga, pembekal, dan pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT.
- ii. Pelaksanaan polisi adalah di bawah tanggungjawab pihak pengurusan PSUK Selangor.

PERANAN

CDO, ICTSO.

1.1.2 Pengesahan Polisi

(Validation of Policy)

Pernyataan

Polisi ini perlu diperakui oleh Jawatankuasa Tadbir Urus Keselamatan Siber PSUK Selangor yang terdiri daripada CDO dan ahli-ahli yang dilantik serta disokong oleh prosedur keselamatan semasa yang sedang berkuat kuasa.

PERANAN

Jawatankuasa Tadbir Urus Keselamatan Siber Pejabat SUK Selangor

1.1.3 Pematuhan Polisi

(Enforcement of Policy)

Pernyataan

- i. PKS mestilah dipatuhi oleh warga, pembekal dan pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT di bawah PSUK dan PDT Selangor.
- ii. Sebarang pelanggaran, ketidakpatuhan dan ketidakakuran pelaksanaan kepada polisi ini hendaklah dilaporkan dengan kadar segera bagi mengekang kesalahan terus berlaku.
- iii. Pihak-pihak yang terlibat boleh dikenakan tindakan tatatertib termasuk sebarang remedi/tindakan undang-undang lain di bawah akta/peraturan/undang-undang semasa yang sedang berkuat kuasa.

PERANAN

ICTSO, Ketua Jabatan, warga SUK dan PDT Selangor, Pembekal dan Pihak Ketiga.

1.1.4 Semakan Polisi Keselamatan Maklumat

(Information Security Policy Review)

Pernyataan

- i. Polisi Keselamatan Maklumat diterjemahkan oleh PSUK Selangor sebagai Polisi Keselamatan Siber (PKS) perlu disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan, dan polisi Kerajaan bagi memastikan kesesuaian, kecukupan dan keberkesananannya berterusan.
- ii. Cadangan pindaan polisi perlu dipertimbangkan dan diperakui oleh Jawatankuasa Tadbir Urus Keselamatan Siber PSUK Selangor bagi tujuan pengesahan.

PERANAN

Bahagian Pengurusan Maklumat (BPM)

1.1.5 Penyebaran Polisi

(Policy Dissemination)

Pernyataan

- i. Program kesedaran tentang PKS hendaklah diatur dan diselaraskan.
- ii. Memaklumkan pindaan yang telah diluluskan oleh JPICT kepada warga PSUK dan PDT Selangor serta semua pihak yang terlibat dalam perkhidmatan ICT di PSUK Selangor.

PERANAN

ICTSO, Ketua Jabatan.

1.1.6 Penyelenggaraan Polisi (Policy Maintenance)

Pernyataan

- i. Penyelenggaraan dan semakan semula PKS hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau mengikut keperluan.
- ii. Polisi ini perlu disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan, dan polisi Kerajaan bagi memastikan kesesuaian, kecukupan dan keberkesanannya berterusan.
- iii. Semua dokumen atau rekod hendaklah diwujudkan dan diselenggara untuk menyediakan bukti pematuhan kepada keperluan dan operasi berkesan pengurusan keselamatan maklumat.
- iv. Semua dokumen dan rekod hendaklah dilindungi dan dikawal mengikut undang-undang atau arahan/ peraturan/garis panduan semasa yang berkuat kuasa.

PERANAN

ICTSO, Ketua Jabatan, warga SUK dan PDT Selangor, Pembekal dan Pihak Ketiga.



SEKSYEN 2

TATA KELOLA

Governance

TATA KELOLA

GOVERNANCE

2.1 (A.5.2) Peranan dan Tanggungjawab Keselamatan Maklumat (Information Security Roles and Responsibilities)

Semua peranan dan tanggungjawab keselamatan maklumat hendaklah ditakrifkan dan diperuntukkan mengikut keperluan.

Objektif: Menerangkan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur bagi mencapai objektif PKS.

Peranan dan Tanggungjawab Keselamatan Maklumat ialah seperti yang berikut:

2.1.1 Jawatankuasa Tadbir Urus Keselamatan Siber PSUK Selangor (JTUKS)

JTUKS PSUK Selangor merupakan jawatankuasa yang bertanggungjawab dalam keselamatan siber yang berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan siber. Keanggotaan JTUKS adalah seperti berikut:



Pengerusi: Timbalan Setiausaha Kerajaan Negeri Selangor
(Pengurusan)

Ahli-ahli:

- a. Timbalan Pegawai Kewangan Negeri
- b. Setiausaha Bahagian (Pengurusan Maklumat)
- c. Setiausaha Bahagian (Khidmat Pengurusan)
- d. Setiausaha Bahagian (Pengurusan Sumber Manusia)
- e. Setiausaha Bahagian (Korporat)
- f. Ketua Penolong Setiausaha Kanan, Bahagian Pengurusan Maklumat
- g. Timbalan Pengarah Seksyen Agihan dan Pembangunan, UPEN
- h. Timbalan Pengarah Seksyen Makro dan Penswastaaan, UPEN
- i. Penolong Pengarah IT, Jabatan Agama Islam Selangor
- j. Ketua Penolong Setiausaha (Kewangan), Bahagian Khidmat Pengurusan
- k. Pegawai Keselamatan ICT (ICTSO), Pejabat SUK Selangor
- l. Ketua Penolong Pengarah IT, Pejabat Tanah dan Galian Selangor
- m. Pengarah IT, Majlis Bandaraya Shah Alam
- n. Pengarah IT, Majlis Bandaraya Petaling Jaya
- o. Pengarah IT, Majlis Perbandaran Subang Jaya
- p. Pengarah IT, Majlis Perbandaran Selayang
- q. Pengarah IT, Majlis Perbandaran Ampang Jaya
- r. Ketua Penolong Setiausaha, Bahagian Pengurusan Maklumat
- s. PSU Kanan Bahagian Pengurusan Maklumat
- t. Ketua-Ketua Unit, Bahagian Pengurusan Maklumat

Urus setia:

Unit Keselamatan & Rangkaian, Bahagian Pengurusan Maklumat.



Bidang kuasa jawatankuasa adalah seperti berikut:

- i. Menyemak dan meluluskan polisi keselamatan siber serta memastikan semakan dibuat sekurang-kurangnya sekali setahun atau apabila berlaku perubahan ketara.
- ii. Menyemak dan meluluskan polisi serta prosedur keselamatan siber bagi memastikan ia selaras dengan keperluan semasa.
- iii. Menyemak dan meluluskan keperluan keselamatan siber bagi setiap perisian dan sistem/aplikasi sebelum kelulusan perolehan
- iv. Menyemak dan meluluskan prosedur Pengurusan Identiti dan Akses (IAM) bagi memastikan keselarasan dengan objektif Entiti NCII serta kecukupan peruntukan sumber.
- v. Menyemak laporan keselamatan siber yang merangkumi kemajuan pencapaian objektif, isu yang dikenal pasti dan keperluan sumber.
- vi. Menyemak dan mengambil maklum laporan audit keselamatan siber serta memastikan tindakan pembetulan dilaksanakan.
- vii. Memperakukan dan mengambil maklum keputusan penilaian risiko yang telah didokumentasikan.
- viii. Memperakukan dan mengambil maklum keputusan rawatan risiko serta memastikan ia dimaklumkan kepada pihak berkepentingan yang berkaitan.
- ix. Mengarahkan dan menyelaraskan pelaksanaan latihan, ujian dan simulasi berasaskan senario sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.
- x. Menyemak dan mengesahkan laporan pematuhan CoP bagi memastikan tahap pematuhan dipatuhi.
- xi. Mengkaji semula, mengemas kini dan memperkukuh polisi, kawalan serta program latihan keselamatan siber berdasarkan risiko baharu dan keperluan pematuhan.

2.1.2 Pasukan Tindak Balas Insiden Keselamatan Siber

Selangor/ Cyber Security Incident Response Team Selangor (CSIRT)

CSIRT ditubuhkan bagi membantu mengendalikan insiden keselamatan ICT, mengawasi dan memberi nasihat berkaitan keselamatan ICT kepada agensi-agensi di bawah kawalannya.

Keanggotaan CSIRT adalah seperti berikut:

Pengerusi : *Chief Digital Officer* (CDO)

Pengurus : *ICT Security Officer* (ICTSO)

- a) Setiausaha Bahagian;
- b) Ketua Penolong Setiausaha Kanan;
- c) Ketua Penolong Setiausaha;
- d) Penolong Setiausaha Kanan;
- e) Semua PSU atau Ketua Unit;
- f) Penolong Pegawai Teknologi Maklumat Kanan/PPTM (mengikut keperluan);
- g) Semua PPTM (Daerah) Selangor;
- h) ICTSO Jabatan-jabatan di bawah pentadbiran Kerajaan Negeri Selangor (Jabatan berkaitan); dan
- i) ICTSO PBT Selangor

Peranan dan tanggungjawab CSIRT adalah seperti berikut:

- i. Menerima dan mengesan aduan keselamatan siber serta menilai tahap dan jenis insiden.
- ii. Merekod dan menjalankan siasatan awal bagi insiden yang diterima.
- iii. Menangani tindak balas insiden keselamatan siber dan mengambil tindakan pemulihan minimum.
- iv. Menasihati agensi di bawah Pentadbiran PSUK Selangor supaya mengambil tindakan pemulihan dan pengukuhan.
- v. Membuat hebahan berkaitan pengukuhan keselamatan siber kepada Pentadbiran PSUK Selangor.

2.1.3 Setiausaha Kerajaan Negeri Selangor

Setiausaha Kerajaan Negeri Selangor mempunyai peranan dan bertanggungjawab dalam perkara berikut:

- i. Memacu hala tuju dan strategi untuk inisiatif pendigitalan bagi warga; dan
- ii. Melantik CDO dan ICTSO serta memaklumkan pelantikan kepada warga.

2.1.4 Ketua Pegawai Digital atau *Chief Digital Officer* (CDO)

CDO ialah Timbalan Setiausaha Kerajaan Negeri (Pengurusan), Ketua Jabatan atau pegawai yang dilantik. Peranan dan tanggungjawab CDO adalah seperti berikut:

- i. Meneraju inisiatif pendigitalan dalam menyediakan penyampaian perkhidmatan yang memenuhi keperluan dan pengalaman rakyat, selamat, efisien, cerdas dan dipercayai:
 - a. Memacu hala tuju pendigitalan berdasarkan Pelan Strategik Pendigitalan (PSP) PSUK Selangor melalui budaya berpacuan data, berpaksikan rakyat dan reka bentuk perkhidmatan berteraskan keselamatan.
 - b. Mentransformasi penyampaian perkhidmatan digital PSUK Selangor berfokuskan pengalaman pelanggan (*customer experience*) yang berteraskan pendekatan keseluruhan kerajaan (*Whole- of-Government*) melalui inovasi melibatkan perkongsian data, data terbuka dan teknologi keterhadapan.
 - c. Merancang dan menyelaraskan pelan tindakan keselamatan siber bagi memastikan data dan infrastruktur ICT agensi sentiasa dilindungi dari ancaman dalam dan luar.
 - d. Merancang dan menilai keperluan perkhidmatan digital, reka bentuk perkhidmatan dan bajet pembangunan serta bajet mengurus yang diperlukan.

- 
- ii. Menerajui perubahan pendigitalan melalui penggunaan data dan teknologi selaras dengan dasar atau pelan semasa kerajaan:
 - a. Merancang dan memastikan pelaksanaan perubahan pendigitalan selaras dengan dasar atau pelan semasa Kerajaan yang diwajibkan kepada PSP PSUK Selangor.
 - b. Mewujudkan persekitaran dan pembudayaan digital di PSUK Selangor bagi meningkatkan literasi digital dan pemahaman tentang penggunaan teknologi ke arah memperkasa penyampaian perkhidmatan kerajaan digital.
 - iii. Menganggotai dan melaporkan pelaksanaan pendigitalan kepada tadbir urus yang berkaitan:
 - a. Merancang dan memastikan pelaksanaan perubahan pendigitalan adalah selaras dengan dasar atau pelan semasa Kerajaan yang diwajibkan kepada PSP PSUK Selangor.
 - b. Melaporkan pelaksanaan dan status kemajuan transformasi pendigitalan kepada tadbir urus pendigitalan yang berkaitan seperti JPICT PSUK Selangor dan Mesyuarat Kerajaan Digital Negeri Selangor.

2.1.5 Pengurus ICT

Pegawai yang bertanggungjawab menguruskan keselamatan siber meliputi aplikasi, operasi dan rangkaian di bawah kawalannya.

Tanggungjawab Pengurus ICT adalah seperti berikut:

- i. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan pentadbiran PSUK dan PDT Selangor.
- ii. Melaksanakan sistem kawalan capaian warga ke atas aset ICT.
- iii. Melaporkan sebarang perkara atau penemuan mengenai keselamatan siber kepada ICTSO.
- iv. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan siber.
- v. Memastikan warga dan pihak luaran yang terlibat dengan jabatan atau agensi mematuhi dasar, piawaian dan garis panduan keselamatan siber dan seterusnya melaporkan sebarang insiden berkaitan.
- vi. Melaksanakan keperluan PKS dalam operasi semasa seperti berikut:
 - a. Perlaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran.
 - b. Pembelian atau peningkatan perisian dan sistem komputer.
 - c. Perolehan teknologi dan perkhidmatan komunikasi.
 - d. Membangunkan garis panduan, prosedur dan tatacara untuk aplikasi khusus (sekiranya perlu).
 - e. Membangun, mengkaji semula dan mengemas kini pelan kontigensi keselamatan siber.

2.1.6 Pegawai Keselamatan ICT atau *ICT Security Officer (ICTSO)*

ICTSO yang dilantik berperanan dan bertanggungjawab dalam perkara berikut:

- i. Mengurus, menyedia dan melaksanakan keseluruhan program-program keselamatan siber.
- ii. Membantu menguatkuasakan pelaksanaan PKS.
- iii. Memberi penerangan dan pendedahan berkenaan PKS kepada warga.
- iv. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS.
- v. Melaksanakan pengurusan risiko dan keselamatan siber.
- vi. Memantau pengurusan perubahan dalam aspek keselamatan maklumat.
- vii. Menguruskan pelaksanaan audit, kajian semula, merumus tindak balas pengurusan pentadbiran PSUK dan PDT Selangor berdasarkan hasil penemuan dan menyediakan laporan mengenainya.
- viii. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian.
- ix. Melaporkan insiden keselamatan siber kepada CDO dan NACSA sekiranya perlu.
- x. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera.
- xi. Menguruskan pelaksanaan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.
- xii. Bertanggungjawab sebagai koordinator pelan pemulihan bencana atau *Disaster Recovery Plan (DRP)*.

2.1.7 Ketua Jabatan

Peranan dan tanggungjawab seperti berikut:

- i. Memastikan pelaksanaan PKS di peringkat jabatan masing-masing.
- ii. Memastikan aset dan sistem jabatan dilindungi secukupnya.
- iii. Menentukan pegawai yang diberi akses kepada sistem dan maklumat.
- iv. Memastikan latihan dan kesedaran keselamatan dilaksanakan.
- v. Melaporkan insiden keselamatan siber kepada ICTSO.
- vi. Memastikan risiko keselamatan siber jabatan diurus dengan baik.
- vii. Menyokong audit dan aktiviti pematuhan keselamatan siber.

2.1.8 Pemilik Sistem

Peranan dan tanggungjawab seperti berikut:

- i. Mengurus risiko sistem di bawah tanggungjawab
- ii. Memastikan pematuhan kawalan keselamatan sistem
- iii. Mengawal akses pengguna
- iv. Memastikan klasifikasi dan perlindungan data
- v. Memastikan *backup* dan *recovery* dilaksanakan

2.1.9 Pentadbir Keselamatan dan Rangkaian

Peranan dan tanggungjawab seperti berikut:

- i. Memastikan ketersediaan rangkaian setempat (LAN) dan rangkaian luas (WAN) di PSUK dan PDT Selangor.
- ii. Memastikan semua peralatan dan perisian rangkaian dan keselamatan di selenggara.
- iii. Merancang peningkatan infrastruktur, ciri keselamatan dan prestasi rangkaian sedia ada.
- iv. Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil.
- v. Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian.
- vi. Memastikan laluan trafik keluar masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian PSUK dan PDT Selangor secara tidak sah.
- vii. Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian.
- viii. Melaksanakan penilaian tahap keselamatan rangkaian dan sistem ICT (*Security Posture Assessment - SPA*) serta penilaian risiko keselamatan maklumat.

2.1.10 Pentadbir Pangkalan Data

Peranan dan tanggungjawab seperti berikut:

- i. Melaksanakan polisi pengguna pangkalan data berdasarkan PKS.
- ii. Melaksanakan pemantauan dan penyelenggaraan pangkalan data secara berterusan.
- iii. Memastikan aktiviti pentadbiran pangkalan data seperti kawalan capaian dan proses pengemaskinian data dilaksanakan dengan teratur.
- iv. Melaporkan sebarang insiden berkaitan keselamatan pangkalan data kepada ICTSO.

2.1.11 Pentadbir Portal atau Laman Web (Webmaster)

Peranan dan tanggungjawab seperti berikut:

- i. Menerima dan memuat naik kandungan portal atau laman web yang telah disahkan oleh pemilik kandungan.
- ii. Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubah suai antara muka.
- iii. Memantau prestasi capaian dan membuat penilaian portal atau laman web secara berkala.
- iv. Memastikan reka bentuk portal atau laman web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi.
- v. Melaksanakan kawalan keselamatan pengoperasian dan perisian lain di web server.
- vi. Melaksanakan proses *backup* dan *restore* secara berkala.
- vii. Melaporkan sebarang isu pelanggaran keselamatan portal atau laman web kepada ICTSO.

2.1.12 Pentadbir Pusat Data atau Bilik Server

Peranan dan tanggungjawab seperti berikut:

- i. Memastikan persekitaran fizikal dan keselamatan Pusat Data atau *Server Room* dalam keadaan baik dan selamat.
- ii. Memastikan keselamatan data dan sistem aplikasi di dalam Pusat Data atau *Server Room*.
- iii. Melaporkan sebarang pelanggaran keselamatan Pusat Data atau *Server Room* kepada ICTSO.

2.1.13 Pentadbir Sistem Aplikasi

Peranan dan tanggungjawab seperti berikut:

- i. Mengkaji cadangan pembangunan atau penyelenggaraan sistem.
- ii. Membuat kajian semula serta menambah baik sistem sedia ada.
- iii. Membuat pemantauan dan penyelenggaraan terhadap sistem.
- vi. Bertanggungjawab dalam aspek pelaksanaan keseluruhan sistem.
- v. Menyediakan dokumentasi sistem yang berkaitan.
- vi. Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas.
- vii. Memastikan kod program sistem aplikasi selamat daripada penggodaman sebelum sistem tersebut diaktifkan untuk penggunaannya.
- viii. Mematuhi dan melaksanakan prinsip PKS dalam pewujudan akaun pengguna ke atas setiap sistem aplikasi.
- ix. Melaporkan kepada ICTSO jika berlaku insiden keselamatan ke atas sistem aplikasi di bawah seliaannya.

2.1.14 Pentadbir Server

Peranan dan tanggungjawab dalam perkara berikut:

- i. Mentadbir, mengurus, menyelenggara dan memantau operasi server termasuk *server* fizikal, pelayan maya (*virtual server*) dan perkhidmatan pengkomputeran awan yang digunakan oleh PSUK dan PDT Selangor;
- ii. Memastikan konfigurasi *server* dilaksanakan secara selamat serta mematuhi keperluan PKS dan garis panduan keselamatan yang berkuat kuasa;
- iii. Melaksanakan pengurusan tampalan keselamatan (*security patch*), kemas kini sistem dan penyelenggaraan *server* secara berkala bagi mengurangkan risiko kerentanan;
- iv. Memastikan kawalan akses ke atas *server* dilaksanakan dengan teratur dan hanya diberikan kepada pengguna yang dibenarkan mengikut keperluan tugas;
- v. Memantau prestasi *server* dan memastikan ketersediaan perkhidmatan sentiasa berada pada tahap optimum;
- vi. Melaksanakan proses sandaran (*backup*) dan pemulihan (*restore*) data server mengikut jadual yang telah ditetapkan;
- vii. Merekod dan memantau log aktiviti *server* bagi tujuan pengauditan dan pengesanan insiden keselamatan;
- viii. Melaporkan sebarang insiden, kelemahan atau pelanggaran keselamatan berkaitan server kepada ICTSO dengan kadar segera; dan
- ix. Bekerjasama dengan pihak berkaitan dalam melaksanakan pelan pemulihan bencana (*Disaster Recovery Plan* – *DRP*) serta memastikan kesiapsiagaan pemulihan sistem.

2.1.15 Pentadbir E-mel

Peranan dan tanggungjawab seperti berikut:

- i. Pengurusan Akaun dan Capaian:
 - a) Mengendalikan permohonan baharu, pengemaskinian dan penutupan akaun pengguna bagi kakitangan yang bertukar/bersara/melanggar dasar dan polisi setelah mendapat kelulusan.
 - b) Mengkonfigurasi kebenaran akses bagi peti mel kongsi dan menetapkan delegasi untuk setiap individu.
- ii. Keselamatan dan Pemantauan:
 - a) Memantau sistem daripada penyalahgunaan, mengesan virus atau perisian hasad serta menapis e-mel spam dan e-mel kuarantin.
- iii. Pematuhan Dasar:
 - a) Menguatkuasakan garis panduan dan etika penggunaan e-mel jabatan termasuk menyiasat sebarang pelanggaran etika seperti penghantaran maklumat sulit secara tidak sengaja atau memuat turun lampiran yang dilarang.
- iv. Sokongan Teknikal:
 - a) Menyelesaikan masalah teknikal berkaitan dengan penghantaran, penerimaan atau konfigurasi pelayan e-mel.

2.1.16 Pegawai Aset

Pegawai yang dilantik oleh Pegawai Pengawal atau Ketua Pengerusi Jawatankuasa Pengurusan Aset Kerajaan (JKPAK) peringkat jabatan atau agensi yang bertanggungjawab menguruskan aset kerajaan berdasarkan pekeliling yang sedang berkuat kuasa.

Peranan dan tanggungjawab seperti berikut:

- i. Mengurus dan memastikan semua aset organisasi direkod, dipantau, dilindungi dan dilupuskan mengikut peraturan yang berkuat kuasa serta keperluan keselamatan maklumat organisasi.
- ii. Memantau perkakasan ICT yang diagihkan kepada warga.

2.1.17 Warga

Peranan dan tanggungjawab seperti berikut:

- i. Membaca, memahami dan mematuhi PKS.
- ii. Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakannya.
- iii. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat.
- iv. Melaksanakan prinsip PKS dan menjaga kerahsiaan maklumat pentadbiran PSUK Selangor.
- v. Tidak membuat pendedahan maklumat terperingkat kepada pihak yang tidak berkenaan.
- vi. Memastikan keabsahan maklumat
- vii. Menjaga kerahsiaan kata laluan.
- viii. Mematuhi piawaian, prosedur dan garis panduan keselamatan siber serta pekeliling atau arahan semasa yang sedang berkuat kuasa.

- ix. Mengaplikasikan pembudayaan keselamatan siber dalam tugas harian.
- x. Menandatangani Surat Akuan Pematuhan PKS seperti di Lampiran 1.
- xi. Mematuhi dan menandatangani Perakuan Akta Rahsia Rasmi 1972 dalam sebarang penyampaian maklumat melalui pelbagai medium komunikasi.
- xii. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera.

2.2 (A.5.3) Pengasingan Tugas *(Segregation of Duties)*

Objektif: Pengasingan tugas dan bidang tanggungjawab dilaksanakan bagi mengurangkan peluang pengubahsuaian data dan maklumat tanpa kebenaran, atau perubahan atau penyalahgunaan aset yang tidak disengajakan.

Pernyataan

- i. Warga SUK dan PDT bertanggungjawab seperti berikut:
 - a) Menyemak, memahami dan mematuhi tanggungjawab keselamatan masing-masing. Sekiranya tidak jelas, pekerja hendaklah mendapatkan penjelasan daripada penyelia;
 - b) Melindungi aset (contohnya maklumat, sumber dan reputasi); dan
 - c) Tugas yang bercanggah serta bidang tanggungjawab hendaklah diasingkan bagi mengurangkan peluang pengubahsuaian atau penyalahgunaan aset secara tidak sah atau tidak disengajakan.

ii. ICTSO, Pengurus ICT dan Pentadbir Sistem ICT bertanggungjawab seperti berikut:

- a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas Aset ICT;
- b) Tugas mewujudkan, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat atau di manipulasi; dan
- c) Persekitaran perkakasan yang digunakan bagi tujuan pembangunan sistem aplikasi (*development/staging*) dan penggunaan sebenar (*production*) hendaklah diasingkan.

2.3 (A.5.4) Tanggungjawab Pengurusan (*Management Responsibilities*)

Objektif: Untuk memastikan pihak pengurusan memahami mereka dalam keselamatan maklumat serta mengambil tindakan bagi memastikan semua personel sedar dan memenuhi tanggungjawab keselamatan maklumat.

Pernyataan

- i. Pelaksanaan polisi ini akan dijalankan oleh CDO dengan disokong oleh JTUKS yang terdiri daripada ICTSO, Ketua Jabatan dan ahli-ahli yang dilantik oleh PSUK Selangor.
- ii. Pengurusan hendaklah memastikan semua warga, pembekal, pihak ketiga dan pihak yang mempunyai urusan dengan perkhidmatan ICT supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.

PERANAN

JTUKS, Pengurus ICT, Ketua Jabatan.

2.4 (A.5.5) Hubungan dengan Pihak Berkuasa

(Contact with Authorities)

Objektif: Untuk memastikan aliran maklumat yang sesuai berkaitan keselamatan maklumat antara organisasi dan pihak berkuasa perundangan, kawal selia dan penyeliaan yang berkaitan.

Pernyataan

Mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan dan bertanggungjawab:

- i. Mewujudkan dan mengemas kini prosedur atau senarai pihak berkuasa perundangan atau pihak yang dihubungi semasa kecemasan. Antara pihak berkuasa perundangan ialah NACSA, Polis Diraja Malaysia dan Suruhanjaya Komunikasi dan Multimedia. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba, penyedia perkhidmatan telekomunikasi dan perkhidmatan bekalan air; dan
- ii. Insiden keselamatan maklumat hendaklah dilaporkan tepat pada masanya bagi mengurangkan impak insiden dan tidak berkompromi kepada sebarang aktiviti pelanggaran ke pihak berkaitan seperti Agensi Keselamatan Siber (NACSA) selaras dengan Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022 bagi mengurangkan impak insiden.

PERANAN

CDO, ICTSO.

2.5 (A.5.6) Hubungan dengan Kumpulan Berkepentingan Khas

(Contact with Special Interest Groups)

Objektif: Untuk memastikan aliran maklumat yang sesuai berkaitan keselamatan maklumat.

Pernyataan

- Mewujudkan dan mengekalkan hubungan dengan kumpulan
- i. berkepentingan khusus, forum keselamatan khusus, serta persatuan profesional.
Keahlian dalam kumpulan atau forum tersebut hendaklah
 - ii. dipertimbangkan sebagai satu kaedah untuk:
 - Meningkatkan pengetahuan berkaitan amalan terbaik (*best practices*);
 - Sentiasa mengikuti perkembangan maklumat keselamatan terkini;
 - Menerima amaran awal berkaitan ancaman, nasihat keselamatan (*advisories*) dan tampalan (*patches*) berkaitan serangan dan kerentanan; dan
 - Mendapatkan akses kepada kepakaran dalam bidang keselamatan maklumat.

PERANAN

CDO, ICTSO, Ketua Jabatan.

2.6 (A.5.8) Keselamatan Maklumat dalam Pengurusan Projek

(Information Security in Project Management)

Objektif: Untuk memastikan risiko keselamatan maklumat yang berkaitan dengan projek dan hasil kerja (*deliverables*) ditangani secara berkesan sepanjang kitar hayat projek.

Pernyataan

Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek tanpa mengira kerumitan, saiz, tempoh, disiplin atau kawasan aplikasinya.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

- i. Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek PSUK dan PDT Selangor;
- ii. Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;
- iii. Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan;
- iv. Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam PKS;
- v. Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak berkaitan yang mempunyai pengetahuan keselamatan maklumat;
- vi. Kesesuaian pertimbangan dan aktiviti keselamatan maklumat hendaklah disusuli pada peringkat yang telah ditetapkan seperti Jawatankuasa Teknikal Projek atau Jawatankuasa Pemandu Projek atau jawatankuasa yang setara; dan
- vii. Peranan dan tanggungjawab keselamatan maklumat projek hendaklah ditakrif dan ditentukan.

PERANAN

ICTSO, CSIRT, Warga PSUK dan PDT Selangor, Pasukan Projek.

2.7 Analisis dan Spesifikasi Keperluan Keselamatan Maklumat (Information Security Requirements Analysis and Specifications)

Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada.

Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut:

- i. Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk konsep perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penyelenggaraan dan pelupusan;
- ii. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan PKS PSUK Selangor;
- iii. Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan
- iv. Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data.

PERANAN

Pentadbir Sistem ICT, Pembekal dan Pihak Ketiga.

2.7 (A.5.35) Kajian Semula Keselamatan Maklumat Secara Berkecuali (Independent Review of Information Security)

Objektif : Untuk memastikan kesesuaian, kecukupan dan keberkesanan berterusan pendekatan organisasi dalam mengurus keselamatan maklumat.

Pernyataan

- i. Pematuhan teknikal secara berkala, seperti ujian penembusan (*penetration test*), penilaian tahap keselamatan (*security posture assessment*), atau kaedah setara, hendaklah dilakukan bagi mengesahkan pematuhan terhadap piawaian pelaksanaan keselamatan.
- ii. Pengurusan dan pelaksanaan keselamatan maklumat oleh pembekal dan pihak ketiga hendaklah dilaksanakan pada sela masa yang dirancang atau apabila berlaku perubahan yang ketara terhadap sistem dan infrastruktur.

PERANAN

CDO, ICTSO, BPM.



SEKSYEN 3

KESELAMATAN SUMBER MANUSIA

Protection of Resources

KESELAMATAN SUMBER MANUSIA

PROTECTION OF RESOURCES

3.1 (A.6.1) Tapisan Keselamatan

(Security Screening)

Objektif: Untuk memastikan warga, pembekal dan pihak ketiga memahami tanggungjawab mereka serta sesuai dengan yang dipertimbangkan.

Pernyataan

- i. Pematuhan teknikal secara berkala, seperti ujian penembusan (*penetration test*), penilaian tahap keselamatan (*security posture assessment*), atau kaedah setara, hendaklah dilakukan bagi mengesahkan pematuhan terhadap piawaian pelaksanaan keselamatan.
- ii. Pengurusan dan pelaksanaan keselamatan maklumat oleh pembekal dan pihak ketiga hendaklah dilaksanakan pada sela masa yang dirancang atau apabila berlaku perubahan yang ketara terhadap sistem dan infrastruktur.

PERANAN

BKP, Warga SUK dan PDT Selangor, Pembekal, Pihak Ketiga.

3.2 (A.6.2) Terma dan syarat perkejaan

(Terms and Conditions of Employment)

Objektif: Untuk memastikan personel memahami tanggungjawab keselamatan maklumat bagi mereka.

Pernyataan

Perkara yang perlu dipatuhi adalah seperti berikut:

- i. Pematuhan teknikal secara berkala, seperti ujian penembusan (*penetration test*), penilaian tahap keselamatan (*security posture assessment*), atau kaedah setara, hendaklah dilakukan bagi mengesahkan pematuhan terhadap piawaian pelaksanaan keselamatan.
- ii. Warga hendaklah membaca, memahami dan menandatangani Surat Akuan Pematuhan PKS PSUK Selangor.
- iii. Warga, pembekal dan pihak ketiga perlu menjalani tapisan keselamatan sekiranya perlu.
- iv. Pembekal atau pihak ketiga perlu menandatangani Surat Akuan Pematuhan PKS, *Non-Disclosure Agreement* (NDA), dan Perakuan Akta Rahsia Rasmi 1972.
- v. Warga, pembekal dan pihak ketiga perlu patuh kepada semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

PERANAN

ICTSO, Warga SUK dan PDT Selangor, Pembekal, Pihak Ketiga.

3.3 (A.6.3) Kesedaran Keselamatan Maklumat, Pendidikan Dan Latihan

(Information Security Awareness, Education and Training)

Objektif: Untuk memastikan warga dan pihak berkepentingan yang berkaitan sedar dan memenuhi tanggungjawab keselamatan maklumat mereka.

Pernyataan

- i. Warga, pembekal atau pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai PKS, sistem pengurusan keselamatan maklumat dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan.

ii. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut:

- a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas Aset ICT;
- b) Memastikan kesedaran yang berkaitan PKS perlu diberi dari masa ke semasa; dan
- c) Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.

PERANAN

ICTSO, Warga SUK dan PDT Selangor, Pembekal atau Pihak Ketiga.

3.4 (A.6.4) Proses Disiplin

(Disciplinary Process)

Objektif : Untuk memastikan personel dan pihak berkepentingan memahami implikasi pelanggaran polisi keselamatan maklumat, serta untuk mencegah dan menangani pelanggaran dengan sewajarnya.

3.4.1 Proses Tatatertib

Pernyataan

Proses tatatertib yang formal perlu ditentukan dan disampaikan kepada warga atau pihak ketiga atau pembekal bagi membolehkan tindakan diambil ke atas pelanggaran keselamatan maklumat yang dilakukan.

PERANAN

Unit Integriti, BPSM.

3.4.2 Tindakan Pemantauan

Pernyataan

Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut:

- i. Memastikan pemantauan dan penguatkuasaan dilaksanakan secara berterusan.
- ii. Memastikan tindakan perundangan dan tatatertib diambil sekiranya berlaku pelanggaran ke atas sebarang peraturan yang berkuat kuasa berkaitan dengan keselamatan siber.

PERANAN

CDO, ICTSO.

3.5 (A.6.5) Penamatan atau pertukaran tanggungjawab perkhidmatan

(Termination or Change of Employment Responsibilities)

Objektif: Untuk melindungi kepentingan organisasi sebagai sebahagian daripada proses perubahan atau penamatan pekerjaan atau kontrak.

Pernyataan

- i. Peranan dan tanggungjawab berkaitan keselamatan maklumat yang masih sah selepas penamatan atau pertukaran perjawatan hendaklah ditentukan, dikuatkuasakan dan disampaikan kepada warga, pembekal, pihak ketiga dan pihak berkepentingan.
- ii. Perkara yang perlu dipatuhi adalah seperti berikut:
 - a) Memastikan semua aset ICT dikembalikan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan;
 - b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan

- c) Pihak ketiga perlu menandatangani Perakuan Untuk Ditandatangani Komuniti Keselamatan atau Mana-Mana pihak lain yang berurusan dengan perkhidmatan awam atau yang berkhidmat di kediaman rasmi kerajaan apabila tamat kontrak perkhidmatan dengan kerajaan berkaitan dengan Akta Rahsia Rasmi 1972 [Akta 88].

PERANAN

ICTSO, Ketua Jabatan, BPSM, Pentadbir Sistem ICT, Pegawai Aset, Warga SUK dan PDT Selangor.

3.6 (A.6.6) Perjanjian Kerahsiaan atau Ketakdedahan

(Confidentiality or Non-Disclosure Agreements)

Objektif: Untuk mengekalkan kerahsiaan maklumat yang boleh diakses oleh kakitangan atau pihak luar.

Pernyataan

Perkara yang perlu dipatuhi adalah seperti berikut:

- i. Syarat-syarat perjanjian kerahsiaan atau *non-disclosure agreement* (NDA) perlu mengambil kira keperluan organisasi dan hendaklah dikenal pasti, didokumentasikan, disemak secara berkala dan ditandatangani oleh warga dan pihak lain yang terlibat dan berkepentingan.
- ii. Pihak berkepentingan hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.
- iii. Perjanjian kerahsiaan dan ketakdedahan bagi setiap pembekal atau pihak berkepentingan yang terlibat dengan perkhidmatan ICT perlu disemak secara berkala sekurang-kurangnya sekali dalam tempoh setahun bagi memastikan senarai pihak pembekal atau pihak yang terlibat dengan perkhidmatan ICT.

PERANAN

Warga SUK dan PDT Selangor, Pihak Ketiga, Pembekal.



SEKSYEN 4

PENGURUSAN PEMBEKAL

Supplier Relationships

PENGURUSAN PEMBEKAL

SUPPLIER RELATIONSHIPS

4.1 (A.5.19) Keselamatan Maklumat dalam Hubungan Pembekal

(Information Security in Supplier Relationships)

Objektif : Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dalam hubungan dengan pembekal.

Pernyataan

- i. Keperluan keselamatan maklumat hendaklah ditakrifkan, dilaksanakan, dipersetujui dan didokumentasikan dengan pembekal atau pihak ketiga bagi mengurangkan risiko kepada aset maklumat
- ii. Pembekal perlu mematuhi arahan keselamatan yang sedang berkuat kuasa. Mengenal pasti dan melaksanakan proses dan prosedur bagi mengurus risiko yang berkaitan dengan penggunaan produk dan perkhidmatan pembekal termasuk penamatan penggunaan produk dan perkhidmatan pembekal.

PERANAN

ICTSO, Ketua Jabatan, Pengurus Projek, Pembekal, Pihak Ketiga.

4.2 (A.5.20) Menangani Keselamatan Maklumat Dalam Perjanjian

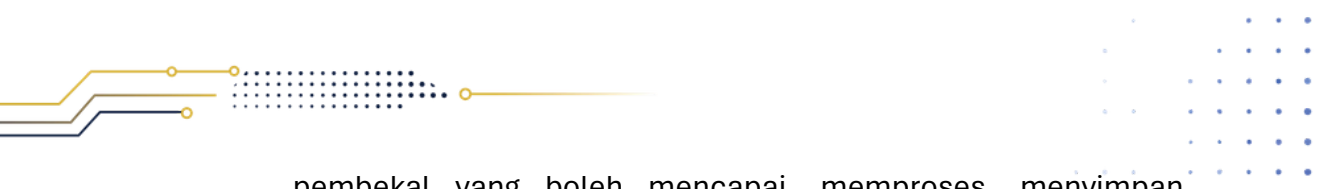
Pembekal

(Addressing Information Security Within supplier Agreements)

Objektif : Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dalam hubungan dengan pembekal.

Pernyataan

- i. Semua keperluan keselamatan maklumat yang berkaitan hendaklah ditakrifkan, disediakan dan dipersetujui dengan setiap



pembekal yang boleh mencapai, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat PSUK Selangor.

- ii. Pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak jabatan selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.
- iii. Sekiranya pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak PSUK Selangor mempunyai kuasa untuk menghalang pembekal daripada melaksanakan perkhidmatan tersebut.

Perkara yang perlu dipatuhi adalah seperti yang berikut:

- a) Memastikan semua aset ICT dikembalikan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan;
- b) Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan;
- c) Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada jabatan berkaitan;
- d) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi;
- e) Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal;
- f) Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut:
 - a) Badan penilai pihak ketiga adalah bebas dan berintegriti;
 - b) Badan penilai pihak ketiga adalah kompeten;
 - c) Kriteria penilaian;

- d) Parameter pengujian; dan
- e) Andaian yang dibuat berkaitan dengan skop penilaian.
- g) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mencapai, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan PSUK atau PDT bagi perjanjian kerahsiaan atau ketakdedahan maklumat dan Perakuan Akta Rahsia Rasmi 1972 (Akta 88); dan
- h) Pembekal hendaklah mematuhi pengelasan maklumat yang telah ditetapkan oleh PSUK.

PERANAN

ICTSO, Ketua Jabatan, Pengurus Projek, Pembekal, Pihak Ketiga.

4.3 (A.5.21) Menguruskan Keselamatan Maklumat dalam Rantaian Bekalan ICT

(Managing Information Security in the ICT Supply Chain)

Objektif: Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dalam hubungan dengan pembekal.

Pernyataan

- i. Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk.
- ii. Pengurusan keselamatan maklumat hendaklah mematuhi perkara berikut:
 - a) Perjanjian dengan pembekal atau pihak ketiga hendaklah diwujudkan dan didokumenkan bagi mengelakkan sebarang salah faham berkaitan tanggungjawab kedua-dua pihak dalam memenuhi keperluan keselamatan maklumat;

- b) PSUK Selangor hendaklah meminta pembekal atau pihak ketiga menyediakan maklumat berkaitan fungsi keselamatan yang dilaksanakan dalam produk mereka serta konfigurasi yang diperlukan untuk operasi yang selamat; dan
- c) Proses pemantauan serta kaedah yang bersesuaian hendaklah dilaksanakan bagi mengesahkan bahawa produk dan perkhidmatan yang diterima mematuhi keperluan keselamatan yang ditetapkan.

PERANAN

ICTSO, Ketua Jabatan.

4.4 (A.5.22) Pemantauan, Semakan dan Pengurusan Perubahan Perkhidmatan Pembekal (*Monitoring, Review and Change Management of Supplier Services*)

Objektif: Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal atau pihak ketiga.

4.4.1 Memantau dan Mengkaji Semula Perkhidmatan Pembekal (*Monitoring and Review Supplier Services*)

Pernyataan

Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal atau pihak ketiga PSUK dan PDT Selangor hendaklah dipantau, disemak dan dinilai secara berkala.

PERANAN

Ketua Jabatan, Pembekal, Pemilik Projek.

4.4.2 Menguruskan Perubahan Kepada Perkhidmatan Pembekal (Managing Changes to Supplier Services)

Pernyataan

- i. Sebarang perubahan terhadap penyediaan perkhidmatan oleh pembekal atau pihak ketiga kepada PSUK dan PDT Selangor hendaklah diurus secara sistematik.
- ii. Pengurusan perubahan tersebut, termasuk penyelenggaraan dan penambahbaikan polisi, prosedur serta kawalan keselamatan maklumat, hendaklah mengambil kira tahap kritikal maklumat, sistem dan proses perkhidmatan yang terlibat serta penilaian semula risiko.

PERANAN

Ketua Jabatan, Pengurus ICT, Pemilik Projek, Pembekal, Pihak Ketiga.

4.5 (A.5.23) Keselamatan Maklumat untuk Penggunaan Perkhidmatan Awam

(Information Security for Use of Cloud Services)

Objektif: Untuk menetapkan dan mengurus keselamatan maklumat bagi penggunaan perkhidmatan awan.

Pernyataan

- i. Proses yang bersesuaian bagi keperluan keselamatan perkhidmatan awan hendaklah ditentukan bagi memastikan keselamatan maklumat terjamin.
- ii. Keselamatan maklumat bagi penggunaan perkhidmatan awan hendaklah merangkumi perkara berikut:
 - a) Memastikan kepatuhan terhadap keperluan perundangan, peraturan, garis panduan dan perjanjian kontrak yang berkaitan dengan perkhidmatan pengkomputeran awan seperti dalam rujukan.

- b) Menyemak setiap perjanjian tahap perkhidmatan (*Service Level Agreement* – SLA) serta mendapatkan dan menganalisis laporan audit keselamatan pembekal awan semasa pelaksanaan perkhidmatan awan dan sekurang-kurangnya sekali setiap tahun selepas itu.;
- c) Melaksanakan alat pemantauan bagi ketampakan berpusat (*centralized visibility*) terhadap infrastruktur perkhidmatan awan; dan
- d) Inventori perkhidmatan awan hendaklah diwujudkan dan disemak secara berkala.

PERANAN

ICTSO, Pentadbir Sistem Aplikasi, Pentadbir Pusat data, Pentadbir Keselamatan dan Rangkaian.



SEKSYEN 5

PENGURUSAN ASET

Asset Management

PENGURUSAN ASET

ASSET MANAGEMENT

5.1 (A.5.9) Inventori maklumat dan aset lain yang berkaitan (Inventory of Information and Other Associated Assets)

Objektif: Untuk mengenal pasti maklumat dan aset berkaitan lain milik Kerajaan Negeri Selangor bagi memastikan keselamatan maklumat terpelihara serta pemilikan yang sesuai ditetapkan.

Pernyataan

Inventori maklumat dan aset berkaitan lain hendaklah merangkumi perkara berikut:

- i. Jabatan hendaklah mengenal pasti dan mendokumentasikan aset ICT dengan lengkap.
- ii. Warga bertanggungjawab atas penggunaan semua aset ICT.
- iii. Pengendalian aset ICT hendaklah merujuk peraturan atau pekeliling semasa yang sedang berkuat kuasa;
- iv. Aset yang berkaitan dengan maklumat dan kemudahan pemprosesan maklumat hendaklah dikenal pasti serta inventori aset tersebut hendaklah diwujudkan dan diselenggara;
- v. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pegawai yang dibenarkan sahaja;
- vi. Inventori bagi semua perisian yang dibenarkan hendaklah diselenggara dan dikemas kini untuk mencerminkan bilangan lesen yang tersedia pada setiap masa. Bukti pemilikan lesen hendaklah disimpan; dan

- vii. Pegawai Aset ICT hendaklah mengesahkan penempatan aset ICT.

PERANAN

Pentadbir Sistem ICT, Pegawai Aset, Pegawai Aset ICT, Warga SUK dan PDT Selangor.

5.2 (A.5.10) Penggunaan Yang Dibenarkan bagi Maklumat dan Aset Berkaitan

(Acceptable Use of Information and Other Associated Assets)

Objektif: Untuk memastikan maklumat dan aset berkaitan dilindungi, digunakan dan dikendalikan dengan sewajarnya.

5.2.1 Penggunaan Aset yang Dibenarkan

(Acceptable Use of Assets)

Pernyataan

- i. Peraturan bagi penggunaan yang dibenarkan ke atas maklumat serta aset yang berkaitan dengan maklumat dan kemudahan pemprosesan maklumat hendaklah dikenal pasti, didokumenkan dan dilaksanakan.
- ii. Prosedur pengendalian aset hendaklah dibangunkan dan dilaksanakan selaras dengan skim pengelasan maklumat yang diterima pakai oleh Kerajaan Negeri Selangor.

PERANAN

CDO, ICTSO, Ketua Jabatan.

5.2.2 Pengendalian Aset

(Handling of Assets)

Pernyataan

Aktiviti pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan hendaklah mengambil kira langkah-langkah keselamatan berikut:

- i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan.
- ii. Memeriksa, menyemak maklumat dan menentukan ia tepat dan lengkap.
- iii. Memastikan maklumat sedia untuk digunakan.
- v. Menjaga kerahsiaan kata laluan.
- vi. Mematuhi piawaian, prosedur, tatacara dan garis panduan keselamatan yang dikeluarkan dari semasa ke semasa.
- vii. Memberi perhatian kepada pengendalian maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.

PERANAN

Pentadbir Sistem ICT, Pegawai Aset, Warga SUK dan PDT Selangor.

5.3 (A.5.11) Pemulangan Aset

(Return of Assets)

Objektif : Untuk melindungi aset organisasi sebagai sebahagian daripada proses perubahan atau penamatan pekerjaan, kontrak atau perjanjian.

Pernyataan

Warga bertanggungjawab untuk memulangkan aset ICT kepada Pegawai Aset atau pegawai bertanggungjawab apabila bertukar keluar atau meninggalkan perkhidmatan.

PERANAN

Warga SUK dan PDT Selangor.

5.4 (A.7.10) Storage Media

Objektif: Untuk memastikan hanya pendedahan, pengubahsuaian, pemindahan atau pelupusan maklumat pada media penyimpanan yang dibenarkan sahaja berlaku.

5.4.1 Pengurusan Media Boleh Alih

(Management of Removal Media)

Pernyataan

- i. Memberi perhatian kepada pengendalian maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.

- ii. Memberi perhatian kepada pengendalian maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.
 - a) Prosedur pengurusan media boleh alih hendaklah dilaksanakan selaras dengan skim pengelasan maklumat yang diterima pakai oleh warga;
 - b) Media hendaklah dilupuskan secara selamat apabila tidak lagi diperlukan menggunakan prosedur formal;
 - c) Maklumat yang disimpan dalam media fizikal hendaklah dikekalkan (sebelum pelupusan) dan rekod pelupusan hendaklah disimpan sebagai jejak audit (*audit trail*);
 - d) Peranti yang rosak dan mengandungi data sensitif hendaklah dinilai melalui penilaian risiko bagi menentukan sama ada perlu dimusnahkan secara fizikal berbanding dibaiki atau dilupuskan;
 - e) Semua peralatan yang mengandungi media penyimpanan hendaklah disahkan untuk memastikan data sensitif dan perisian berlesen telah dipadam atau ditulis semula secara selamat sebelum pelupusan atau penggunaan semula; dan
 - f) Media fizikal dan peralatan ICT yang dibawa masuk atau keluar dari premis PSUK Selangor hendaklah tertakluk kepada proses kebenaran dan rekod yang ditetapkan oleh organisasi bagi memastikan keselamatan aset dan maklumat serta mencegah akses tanpa kebenaran, kehilangan, penyalahgunaan atau kerosakan.

PERANAN

Pegawai Aset, Pentadbir Sistem ICT, Warga SUK dan PDT Selangor.

5.4.2 Pelupusan Media

(Disposal Media)

Pernyataan

- i. Pelupusan media mudah alih perlu mendapat kelulusan daripada pegawai-pegawai yang diwakilkan kuasa di bawah Akta Perwakilan Kuasa 1956 boleh meluluskan mengikut had nilai yang ditetapkan dan tidak boleh mewakilkan kuasa kepada mana-mana pegawai lain dan mengikut prosedur kerajaan yang berkenaan.
- ii. Peraturan yang perlu dipatuhi dalam pelupusan media adalah seperti berikut:
 - a) Peranti yang rosak dan mengandungi data sensitif hendaklah dinilai melalui penilaian risiko bagi menentukan sama ada perlu dimusnahkan secara fizikal berbanding dibaiki atau dilupuskan;
 - b) Pelupusan media mudah alih dalam aset ICT hendaklah dilaksanakan mengikut Pekeliling Pengurusan Aset Alih Kerajaan yang berkuat kuasa.

PERANAN

Lembaga Pemeriksa Pelupusan Aset, Pegawai Aset. Pentadbir Sistem ICT, Warga SUK dan PDT Selangor .

5.5 (A.7.13) Penyelenggaraan Peralatan (Equipment Maintenance)

Objektif: Untuk mencegah kehilangan, kerosakan, kecurian atau kompromi maklumat dan aset berkaitan lain serta gangguan kepada operasi organisasi akibat kekurangan penyelenggaraan.

Pernyataan

Peralatan ICT hendaklah diselenggara bagi memastikan kebolehsediaan, kerahsiaan dan integriti data atau maklumat terjamin dengan mengambil langkah-langkah seperti berikut:

- i. Semua peralatan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar.
- ii. Memastikan peralatan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja.
- iii. Pentadbir Sistem ICT bertanggungjawab terhadap setiap peralatan bagi penyelenggaraan peralatan sama ada dalam tempoh jaminan atau telah tamat tempoh jaminan.
- iv. Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan serta memastikan laporan penyelenggaraan disediakan.
- v. Memaklumkan warga sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau mengikut keperluan.

PERANAN

Pentadbir Sistem ICT, Pegawai Aset.

5.6 (A.7.14) Pelupusan atau Penggunaan Semula Peralatan Secara Selamat (Secure Disposal or Re-Use of Equipment)

Objektif: Untuk mencegah kebocoran maklumat daripada peralatan yang akan dilupuskan atau digunakan semula.

Pernyataan

- i. Pelupusan atau penggunaan semula peralatan ICT melibatkan peralatan yang usang, rosak dan tidak boleh dibaiki.
- ii. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa dan perkara yang perlu dipatuhi adalah seperti berikut:
 - a) Peranti yang rosak dan mengandungi data sensitif hendaklah dinilai melalui penilaian risiko bagi menentukan sama ada perlu dimusnahkan secara fizikal berbanding dibaiki atau dilupuskan;
 - b) Sekiranya maklumat perlu disimpan, salinan pendua (*backup*) mestilah dilaksanakan;
 - c) Data-data dalam storan peralatan ICT yang akan dilupuskan secara pindah milik hendaklah dihapuskan dengan cara yang selamat;
 - d) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;
 - e) Pegawai yang dilantik hendaklah merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT dalam senarai inventori mengikut tatacara pengurusan aset atau sistem yang sedang berkuat kuasa; dan
 - f) Pelupusan peralatan ICT hendaklah mengikut tatacara pelupusan semasa yang berkuat kuasa.

- iii. Warga adalah dilarang daripada melakukan perkara seperti berikut:
- a) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi;
 - b) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *Control Processing Unit (CPU)* seperti *RAM*, *hard disk*, *motherboard* dan sebagainya.
 - c) Menyimpan dan memindahkan perkakasan luaran komputer seperti *Automatic Voltage Regulator (AVR)*, *speaker* dan mana-mana peralatan yang berkaitan.
 - d) Melupuskan sendiri peralatan ICT.
 - e) Memindahkan keluar dari premis mana-mana peralatan ICT yang hendak dilupuskan.
 - f) Memastikan segala maklumat sulit dan rahsia di dalam peralatan disalin pada media storan kedua sebelum menghapuskan maklumat secara kekal.

PERANAN

Lembaga Pemeriksa Pelupusan Aset, Pegawai Aset, Pentadbir Sistem ICT, Warga SUK dan PDT Selangor.

5.7 (A.8.1) Peranti Titik Akhir Pengguna

(User Endpoint Devices)

Objektif : Untuk melindungi maklumat daripada risiko yang timbul akibat penggunaan peranti titik akhir pengguna.

Pernyataan

Peranti titik akhir pengguna, termasuk BYOD (*Bring Your Own Device*) yang telah diluluskan, hendaklah mematuhi perkara berikut:

- i. Peranti atau kawasan di mana peranti ditempatkan hendaklah dilindungi secara fizikal (contohnya menggunakan kunci atau kaedah setara) sekiranya ditinggalkan tanpa pengawasan;

- ii. Komputer yang ditinggalkan tanpa pengawasan hendaklah dikunci dengan mengaktifkan mod tidur atau pelindung skrin (contohnya pelindung skrin yang dilindungi kata laluan) yang memerlukan kata laluan untuk mengakses semula sesi;
- iii. Peranti (*hardware*) aset alih ICT didaftarkan oleh Pegawai Aset atau Pegawai yang diberi kuasa dan ditandatangani oleh Ketua Bahagian, Jabatan, Seksyen/ Unit pada KEW.PA3;
- iv. Peranti hendaklah dipasang dengan perisian berlesen dan perisian perlindungan serta dikemas kini secara berkala;
- v. Data yang disimpan dalam peranti peribadi hendaklah dilindungi pada setiap masa;
- vi. Peranti hendaklah dilindungi secara fizikal daripada kecurian (contohnya di tempat awam, kenderaan, bilik hotel, persidangan dan kawasan tidak selamat);
- vii. Aset bukan hak milik PSUK dan PDT Selangor hendaklah didaftarkan dan diurus mengikut polisi/prosedur/arahan-arahan *Bring Your Own Device (BYOD)* yang sedang berkuat kuasa;
- viii. Warga mempunyai hak sepenuhnya untuk mengakses data dalam peranti peribadi bagi tujuan rasmi. Sebarang tindakan seperti membangunkan, menyalin, menyebarkan, melaksanakan atau cuba memperkenalkan virus komputer atau kod berniat jahat yang boleh mereplikasi sendiri, merosakkan atau menjejaskan prestasi komputer atau rangkaian SUK dan PDT Selangor adalah dilarang; dan
- ix. Sebarang peranti yang memerlukan akses Wi-Fi hendaklah mendapat kebenaran daripada ICTSO terlebih dahulu.

PERANAN

ICTSO, Warga SUK dan PDT Selangor.



SEKSYEN 6

PENGURUSAN RISIKO KESELAMATAN MAKLUMAT

*Information Security Risk
Management*

PENGURUSAN RISIKO KESELAMATAN MAKLUMAT

INFORMATION SECURITY RISK MANAGEMENT

6.1 Pengurusan Risiko Keselamatan Maklumat & Strategi Perkhidmatan

(Information Security Risk Management & Service Strategy)

Objektif: Memastikan risiko keselamatan maklumat diurus secara sistematik untuk melindungi kerahsiaan, integriti dan ketersediaan maklumat, sekaligus menyokong pematuhan dan membantu pengurusan membuat keputusan berasaskan risiko.

Pernyataan

- i. Pengurusan risiko keselamatan maklumat mesti diselaraskan dengan proses pengurusan risiko sedia ada, dengan tadbir urus, tanggungjawab dan pelaporan yang jelas dan sistematik.
- ii. Pengurusan risiko perlu mengambil kira penggunaan teknologi AI (termasuk Generative AI, Machine Learning, LLM), automasi pintar dan sistem analitik pintar dalam persekitaran digital organisasi.
- iii. Penggunaan teknologi AI hendaklah tertakluk kepada penilaian risiko keselamatan maklumat, perlindungan data, privasi, integriti maklumat, ketepatan *output* dan pematuhan kepada peraturan serta arahan kerajaan yang berkuat kuasa.
- iv. Sebarang penggunaan platform AI awam atau perkhidmatan AI pihak ketiga hendaklah dinilai dari aspek risiko keselamatan siber, risiko kebocoran data, kedaulatan data dan pematuhan kepada klasifikasi maklumat rasmi kerajaan.

PERANAN

ICTSO, Ketua Jabatan.

6.2 Pengenalpastian dan Penilaian Risiko Keselamatan Maklumat *(Information Security Risk Identification and Assessment)*

Objektif: Memastikan risiko keselamatan maklumat dikenal pasti, dinilai dan diurus secara sistematik bagi melindungi aset maklumat serta menyokong kesinambungan penyampaian perkhidmatan.

Pernyataan

- i. PSUK Selangor hendaklah mengenal pasti, menilai, mendokumenkan dan menyemak risiko keselamatan maklumat secara berkala atau apabila berlaku perubahan yang boleh menjejaskan aset maklumat, sistem ICT atau penyampaian perkhidmatan.
- ii. Hasil penilaian risiko hendaklah dijadikan asas dalam menentukan kawalan keselamatan yang bersesuaian.

6.2.1 Pengenalpastian dan Penilaian

Pernyataan

- i. Pengenalpastian dan Penilaian Risiko Keselamatan Maklumat bagi aset ICT PSUK dan PDT Selangor hendaklah diwujudkan bagi menentukan ancaman yang wujud terhadap sesuatu aset serta tahap risiko yang berkaitan dengan ancaman tersebut.
- ii. Pengenalpastian risiko hendaklah merangkumi ancaman dan kerentanan berkaitan penggunaan AI.
- iii. Penilaian risiko AI hendaklah mengambil kira impak terhadap:
 - a) Kerahsiaan data;
 - b) Integriti maklumat;
 - c) Ketersediaan perkhidmatan;
 - d) Reputasi organisasi;
 - e) Kesinambungan perkhidmatan digital;
 - f) Kedaulatan data kerajaan.

- iv. Sistem atau aplikasi yang menggunakan AI hendaklah dikenal pasti dan direkodkan dalam Daftar Aset serta Daftar Risiko PSUK Selangor.

PERANAN

ICTSO, Ketua Jabatan, Pemilik Sistem.

6.2.2 Pelaksanaan

(Implementation)

Pernyataan

- i. Melaksanakan proses memilih langkah perlindungan dan kawalan yang bersesuaian bagi mengurangkan risiko ke tahap yang boleh diterima. Proses ini hendaklah diselaraskan dengan proses pengukuran risiko.
- ii. Langkah perlindungan dan kawalan keselamatan bagi penggunaan AI hendaklah dilaksanakan berdasarkan tahap risiko yang telah dikenal pasti.
- iii. Kawalan keselamatan AI hendaklah meliputi:
 - a) Kawalan akses;
 - b) Pengelasan data;
 - c) Penggunaan data minimum;
 - d) Pemantauan aktiviti AI;
 - e) Logging dan audit trail;
 - f) Kawalan integrasi API;
 - g) Pengesahan manusia (*human oversight*).
- iv. Data atau maklumat rahsia rasmi PSUK & PDT Selangor yang diklasifikasikan sebagai dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit”, atau “Terhad” dilarang diproses menggunakan platform AI awam tanpa kelulusan rasmi.

PERANAN

ICTSO, Ketua Jabatan, Pemilik Sistem.

6.3 Rawatan Risiko Keselamatan Maklumat

(Information Security Risk Treatment)

Objektif: Memastikan risiko keselamatan maklumat dirawat melalui pelaksanaan kawalan yang bersesuaian bagi mengurangkan impak dan kemungkinan berlakunya risiko ke tahap yang boleh diterima oleh PSUK Selangor.

6.3.1 Pewujudan Proses

(Process Creation)

Pernyataan

- i. Mewujudkan proses Rawatan Risiko Keselamatan Maklumat bagi mengenal pasti tindakan pengurusan yang bersesuaian, sumber, tanggungjawab serta keutamaan dalam mengurus risiko keselamatan maklumat.
- ii. Proses Rawatan Risiko Keselamatan Maklumat hendaklah merangkumi pengurusan risiko berkaitan penggunaan dan pelaksanaan teknologi AI.
- iii. Penggunaan AI bagi fungsi kritikal organisasi hendaklah melalui proses kelulusan dan semakan keselamatan yang bersesuaian.

PERANAN

ICTSO, Ketua Jabatan.

6.3.2 Pelaksanaan

(Implementation)

Pernyataan

- i. Melaksanakan Rawatan Risiko Keselamatan Maklumat dan memantau keberkesanan kawalan keselamatan bagi mengurangkan risiko ke tahap yang boleh diterima. Proses ini hendaklah diselaraskan dengan proses kawalan risiko.

- ii. Rawatan risiko AI hendaklah dilaksanakan secara berterusan bagi memastikan penggunaan AI tidak menjejaskan keselamatan maklumat organisasi.

PERANAN

ICTSO, Ketua Jabatan, Pemilik Sistem.

6.4 Pemantauan Risiko Keselamatan Maklumat

(Information Security Risk Monitoring)

Objektif: Memastikan risiko keselamatan maklumat dipantau dan disemak secara berterusan bagi mengekalkan keberkesanan kawalan keselamatan serta memastikan risiko berada pada tahap yang boleh diterima oleh PSUK Selangor.

Pernyataan

Perkara-perkara yang perlu dilakukan bagi pemantauan risiko keselamatan maklumat adalah seperti yang berikut:

- i. Mengesahkan bahawa langkah tindak balas risiko yang dirancang telah dilaksanakan serta diselaraskan dengan proses Pemantauan Risiko;
- ii. Keperluan keselamatan maklumat yang diperoleh daripada atau boleh dijejak kepada misi PSUK Selangor, fungsi Perkhidmatan, perundangan, arahan, peraturan, polisi, piawaian dan garis panduan hendaklah dipenuhi;
- iii. Pemantauan risiko keselamatan maklumat hendaklah turut meliputi aktiviti penggunaan AI.

PERANAN

ICTSO, Ketua Jabatan.

6.5 Komunikasi Risiko Keselamatan Maklumat (Information Security Risk Communication)

Objektif: Memastikan maklumat berkaitan risiko keselamatan maklumat disampaikan kepada pihak berkepentingan secara tepat, jelas dan tepat pada masanya bagi menyokong pengurusan risiko yang berkesan.

Pernyataan

Perkara-perkara yang perlu dilakukan bagi memastikan komunikasi risiko keselamatan maklumat adalah seperti yang berikut:

- i. Mewujudkan aktiviti Komunikasi Risiko Keselamatan Maklumat dan selaraskannya dengan proses Pelaporan Risiko bagi mencapai persetujuan dalam pengurusan risiko melalui pertukaran dan perkongsian maklumat risiko dengan pemilik risiko dan pihak berkepentingan yang berkaitan; dan
- ii. Maklumat tersebut termasuk, tetapi tidak terhad kepada, kewujudan, sifat, bentuk, kebarangkalian, akibat, kepentingan, rawatan dan penerimaan risiko.
- iii. Komunikasi Risiko Keselamatan Maklumat hendaklah merangkumi kesedaran dan perkongsian maklumat berkaitan risiko penggunaan AI kepada semua warga organisasi, pembekal dan pihak berkepentingan.

Penilaian Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dikaji semula sekurang-kurangnya sekali setahun.

PERANAN

ICTSO, Ketua Jabatan.



SEKSYEN 7

PERLINDUNGAN MAKLUMAT

Information Protection

PERLINDUNGAN MAKLUMAT

INFORMATION PROTECTION

7.1 (A.5.12) Pengelasan Maklumat

(Classification of Information)

Objektif: Untuk memastikan keperluan perlindungan maklumat dikenal pasti dan difahami selaras dengan kepentingannya kepada organisasi.

Pernyataan

- i. Data dan maklumat perlu dikelas oleh Pegawai Pengelas mengikut keperluan keselamatan maklumat yang telah ditetapkan dalam Arahan Keselamatan berdasarkan keperluan perlindungan keselamatan maklumat tersebut.
- ii. Pengelasan maklumat terdiri daripada aktiviti penentuan klasifikasi maklumat serta penentuan peringkat keselamatan maklumat. Klasifikasi maklumat terdiri daripada maklumat rahsia rasmi dan maklumat rasmi manakala peringkat keselamatan maklumat terdiri daripada rahsia besar, rahsia, sulit terhad, data terkawal atau sensitif dan terbuka.
- iii. Perkara di bawah hendaklah dilaksanakan oleh semua pihak yang terlibat dalam pengelasan maklumat:
 - a) Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik oleh PSUK Selangor dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan dalam Arahan Keselamatan;
 - b) Mematuhi piawaian, prosedur, tatacara dan garis panduan keselamatan dan pengendalian maklumat atau dokumen yang sedang berkuat kuasa;
 - c) Memberi perhatian semasa mengendalikan maklumat rahsia terperingkat;
 - d) Memastikan tiada pendedahan maklumat kepada pihak yang tidak dibenarkan;

- e) Pengelasan maklumat adalah berpandukan kepada Arahan Keselamatan (Semakan dan Pindaan 2017), Arkib Negara, Surat Pekeliling Am Bil.2/1987 Peraturan Pengelasan Semula Rekod Terperingkat dan arahan-arahan lain yang berkuat kuasa.
- f) Pengurusan maklumat dan rekod hendaklah berpandukan kepada Akta dan standard berkaitan pengurusan rekod serta pekeliling, arahan, dasar dan garis panduan yang dikeluarkan oleh Pejabat Pegawai Keselamatan Kerajaan dan Arkib Negara Malaysia; dan
- g) Memastikan kesemua fail fizikal dan digital maklumat disimpan mengikut keperluan perlindungan keselamatan yang ditetapkan oleh pihak Kerajaan.

PERANAN

Ketua Jabatan, Pegawai Rekod, Pegawai Pengelas, Pegawai Pengurus Rekod, Pemilik Rekod, Pengguna Rekod.

7.2 (A.5.13) Pelabelan Maklumat

(Labelling of Information)

Objektif: Untuk memudahkan komunikasi tahap pengelasan maklumat serta menyokong automasi pemprosesan dan pengurusan maklumat.

Pernyataan

Perkara-perkara yang perlu dilakukan bagi proses pelabelan maklumat adalah seperti yang berikut:

- i. Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan yang berkuat kuasa; dan
- ii. Pelabelan Maklumat yang melibatkan infrastruktur rangkaian seperti pengkabelan (*wired*) perlu rujuk kepada dokumen L-S38 (*Specification for ICT Networking System*) yang diterbitkan oleh Jabatan kerja Raya (JKR) atau sebarang standard, garis panduan, pekeliling dan arahan yang berkuat kuasa.

PERANAN

Pegawai Rekod, Pegawai Pengelas, Pegawai Pengurus Rekod, Pemilik Rekod, Pengguna Rekod.

7.3 (A.5.14) Pemindahan maklumat

(Information Transfer)

Objektif: Untuk mengekalkan keselamatan maklumat yang dipindahkan dalam organisasi dan dengan pihak berkepentingan luar.

7.3.1 Polisi dan Prosedur Pemindahan Data dan Maklumat

(Information Transfer Policies and Procedures)

Pernyataan

- i. Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi.
- ii. Agensi dan pihak berkepentingan yang terlibat dalam perkongsian data perlu bertanggungjawab sepenuhnya untuk menjaga keselamatan, kerahsiaan dan privasi data ketika proses pemindahan atau pengintegrasian data dengan merujuk kepada Dasar Perkongsian Data Sektor Awam dan Dasar Perkongsian Data Selangor.
- iii. Perkara-perkara yang perlu dilakukan bagi pemindahan maklumat adalah seperti yang berikut:
 - a) Keselamatan maklumat atau menandatangani perjanjian bertulis perlu diambil kira apabila berlaku pemindahan data dan maklumat organisasi dengan pihak luar;
 - b) Terma pemindahan data, maklumat dan perisian antara PSUK Selangor dengan pihak luar hendaklah dimasukkan di dalam Perjanjian;

- c) Media yang mengandungi maklumat rasmi Kerajaan perlu dilindungi;
- d) Sebarang pemindahan maklumat di antara PSUK Selangor dan agensi lain mestilah dikawal; dan
- e) Penggunaan perkhidmatan luar seperti aplikasi media sosial dan perkongsian fail untuk pemindahan maklumat rasmi Kerajaan perlu merujuk Arahan Keselamatan.

PERANAN

CDO, ICTSO, Pemilik Sistem, Pentadbir Sistem ICT, Pemilik Maklumat.

7.3.2 Pemindahan Elektronik

(Electronic Transfer)

Pernyataan

Perkara-perkara berikut perlu dipertimbangkan apabila menggunakan kemudahan komunikasi elektronik untuk pemindahan data dan maklumat:

- i. Pengesanan dan perlindungan terhadap perisian hasad yang boleh dihantar melalui penggunaan komunikasi elektronik;
- ii. Perlindungan maklumat elektronik sensitif yang disampaikan dalam bentuk lampiran;
- iii. Pencegahan penghantaran dokumen dan mesej ke alamat yang salah dalam komunikasi elektronik;
- iv. Mendapatkan kelulusan sebelum menggunakan perkhidmatan awam luar seperti pemesanan segera, rangkaian sosial, perkongsian fail atau storan awan;
- v. Tahap pengesanan yang lebih kukuh apabila memindahkan maklumat melalui rangkaian yang boleh diakses secara umum;
- vi. Sekatan yang berkaitan dengan kemudahan komunikasi secara elektronik seperti mencegah *automatic forwarding* bagi e-mel ke alamat e-mel luar;

- vii. Memberi kesedaran kepada warga PSUK dan PDT Selangor untuk tidak menghantar khidmat pesanan ringkas atau pemesejan segera bagi maklumat kritikal kerana ia berisiko diterima oleh orang yang tidak dibenarkan atau disimpan dalam peranti yang tidak dilindungi secukupnya; dan
- viii. Maklumat yang terlibat dalam pemindahan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa.

PERANAN

Ketua Jabatan, Pentadbir E-mel, Pentadbir Rangkaian, Warga SUK dan PDT Selangor.

7.3.3 Pemindahan Media Storan Fizikal

(Physical Storage Media Transfer)

Pernyataan

- i. Media yang mengandungi maklumat perlu dilindungi daripada akses tanpa izin, penyalahgunaan atau kerosakan semasa dipindahkan. Media yang dimaksudkan juga adalah termasuk dokumen dalam bentuk kertas.
- ii. Pemindahan dokumen terperingkat secara fizikal perlu mengikut prosedur-prosedur seperti di dalam Arahan Keselamatan.

PERANAN

Ketua Jabatan, Pentadbir Pusat Data.

7.4 (A.5.33) Perlindungan Rekod (Protection of Records)

Objektif: Untuk memastikan pematuhan kepada keperluan perundangan, statutori, kawal selia dan kontrak, serta jangkaan komuniti atau masyarakat berkaitan perlindungan dan ketersediaan rekod.

Pernyataan

- i. Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, akses tanpa izin dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.
- ii. Perlindungan rekod mestilah mengikut perkara berikut:
 - a) Rekod yang bersesuaian hendaklah diselenggara bagi menjejak semua aset maklumat termasuk peralatan atau perisian ICT di premis; dan
 - b) Rekod hendaklah disimpan berdasarkan tempoh penyimpanan yang ditetapkan oleh pemilik data dan/atau pemilik sistem.

PERANAN

Warga SUK dan PDT Selangor, Pemilik Sistem, Pemilik Perkhidmatan, Pengurus Projek, Pembekal, Pihak Ketiga.

7.5 (A.8.7) Perlindungan Terhadap Perisian Hasad

(*Protection against Malware*)

Objektif: Untuk memastikan maklumat dan aset berkaitan lain dilindungi daripada perisian hasad (*malware*).

Pernyataan

- i. Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada serangan perisian hasad hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut.
- ii. Perkara yang perlu dilaksanakan bagi memastikan perlindungan aset maklumat daripada perisian hasad ialah seperti yang berikut:
 - a) Memasang sistem keselamatan untuk mengesan perisian atau program perisian hasad seperti antivirus, *Intrusion Detection System (IDS)*, *Intrusion Prevention System (IPS)* dan *Web Application Firewall (WAF)* serta mengikut prosedur penggunaan yang betul dan selamat;
 - b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah undang-undang yang sedang berkuat kuasa;
 - c) Mengimbas semua perisian atau sistem dengan *antivirus* sebelum menggunakannya;
 - d) Mengemas kini *antivirus* dengan *signature/pattern* antivirus yang terkini;
 - e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;
 - f) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;

- g) Menyediakan pelan kesinambungan perkhidmatan yang sesuai untuk pulih daripada serangan perisian hasad;
- h) Menentukan prosedur dan tanggungjawab untuk menangani perlindungan terhadap perisian hasad pada sistem;
- i) Mengesahkan ketepatan sumber maklumat yang berkaitan dengan perisian hasad dan;
- j) Perisian tidak boleh dimuat turun atau dipasang daripada sistem luar PSUK Selangor tanpa kelulusan terlebih dahulu.

PERANAN

Pemilik Aset, Pentadbir Sistem.

7.6 (A.8.10) Pemadaman Maklumat

(Information Deletion)

Objektif: Untuk mencegah pendedahan maklumat sensitif yang tidak perlu serta memastikan pematuhan kepada keperluan perundangan, statutori, kawal selia dan kontrak berkaitan pemadaman maklumat.

Pernyataan

- i. Maklumat terperingkat yang disimpan dalam aset maklumat hendaklah dilupuskan mengikut prosedur yang ditetapkan.
- ii. Perkara yang perlu dipatuhi ialah seperti berikut:
 - a) Menentukan kaedah penghapusan maklumat yang sesuai selaras dengan keperluan PSUK Selangor;
 - b) Merekod keputusan sebagai bukti penghapusan maklumat; dan
 - c) Mendapatkan bukti penghapusan maklumat jika menggunakan perkhidmatan pembekal.

PERANAN

Pemilik Maklumat, Pemilik Aset, Pegawai Aset.

7.7 (A.8.11) Penyamaran Data (Data Masking)

Objektif: Untuk mengehadkan pendedahan data sensitif termasuk Maklumat Pengenalan Peribadi (PII) serta mematuhi keperluan perundangan, statutori, kawal selia dan kontrak.

Pernyataan

Penyembunyian data dilaksanakan bagi melindungi data sensitif seperti data *Personal Identifiable Information* (PII), dan data terperingkat dengan mengambil kira keperluan perkhidmatan dan polisi kawalan capaian serta polisi lain yang berkaitan tertakluk kepada keperluan perundangan dan peraturan yang berkuat kuasa. Pelaksanaan penyamaran data ialah berdasarkan prosedur yang ditetapkan.

Penyembunyian data diperlukan bagi melindungi data PII dan data sensitif daripada terdedah atau bocor kepada pihak yang tidak bertanggungjawab yang akan menyebabkan imej PSUK Selangor terjejas.

Perkara yang perlu dipatuhi ialah seperti yang berikut:

- i. Mengenal pasti klasifikasi data yang perlu dikongsi dengan pihak ketiga;
- ii. Pasti teknik yang sesuai selaras dengan sensitiviti data; dan
- iii. Memastikan pengguna hanya dapat mencapai data minimum yang dibenarkan sahaja.

PERANAN

Pemilik Maklumat, Pentadbir Sistem ICT.

7.8 (A8.12) Pencegahan Ketirisan Data

(Data Leakage Prevention - DLP)

Objektif: Untuk mengesan dan mencegah pendedahan serta pengekstrakan maklumat tanpa kebenaran oleh individu atau sistem.

Pernyataan

- i. Kawalan pencegahan kebocoran maklumat hendaklah dilaksanakan terhadap infrastruktur, sistem, rangkaian dan peralatan-peralatan ICT yang digunakan untuk memproses, menyimpan atau menghantar maklumat terperingkat atau berdarjah bagi mengenal pasti dan mencegah kebocoran maklumat.
- ii. Perkara yang perlu dipatuhi ialah seperti berikut:
 - a) Menenal pasti dan mengelaskan maklumat untuk dilindungi daripada ketirisan;
 - b) Memantau saluran transaksi dan perkongsian data (contohnya e-mel, pemindahan fail, perkhidmatan peranti atau media mudah alih);
 - c) Melaksanakan tindakan pengukuhan untuk mengelakkan ketirisan maklumat; dan
 - d) Melaksanakan tindakan pengukuhan pada peralatan ICT untuk mengurangkan risiko kerentanan.

PERANAN

Pemilik Maklumat, Pentadbir Sistem ICT.

7.9 (A8.33) Maklumat Pengujian

(*Test Information*)

Objektif: Untuk memastikan kesesuaian pengujian serta perlindungan maklumat operasi yang digunakan untuk tujuan ujian.

Pernyataan

- i. Perlindungan ke atas maklumat yang digunakan untuk pengujian, data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal.
- ii. Maklumat ujian hendaklah mematuhi perkara berikut:
 - a) Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal.
 - b) Jenis data yang digunakan untuk tujuan ujian hendaklah ditentukan dan diluluskan oleh pemilik data yang berkaitan;
 - c) Sekiranya pengujian memerlukan penggunaan maklumat pengeluaran (*production*) yang dikelaskan, maklumat tersebut hendaklah dinyah identiti (*sanitized*) bagi memastikan data sensitif tidak didedahkan kepada pihak yang tidak dibenarkan; dan
 - d) Data ujian hendaklah dipadam daripada sistem ujian apabila tidak lagi diperlukan.

PERANAN

Pemilik Maklumat, Pemilik Sistem.

7.10 (A.8.34) Perlindungan Sistem Maklumat Semasa Ujian Audit

(Protection of Information Systems during Audit Testing)

Objektif : Untuk meminimumkan impak aktiviti audit dan jaminan lain terhadap sistem operasi dan proses perkhidmatan.

Pernyataan

- i. Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas fungsi penyampaian perkhidmatan PSUK Selangor.
- ii. Perlindungan sistem maklumat semasa ujian audit hendaklah mematuhi perkara berikut:
 - a) Ciri penjanaan log hendaklah diaktifkan bagi merekod perubahan terhadap maklumat sensitif dalam semua sistem aplikasi pengeluaran (*production*), termasuk setiap penambahan, pengubahsuaian dan pemadaman maklumat; dan
 - b) Log peristiwa keselamatan maklumat hendaklah disemak secara berkala oleh pekerja yang dilantik serta mempunyai pengetahuan dan kemahiran yang bersesuaian. Kekerapan semakan hendaklah bergantung kepada tahap risiko yang terlibat.

PERANAN

Pemilik Maklumat, Pemilik Sistem.

7.11 Penggunaan AI dan Perlindungan Data

(AI Use and Data Protection)

Objektif : Untuk memastikan data dan maklumat rasmi kerajaan dilindungi semasa penggunaan AI.

Pernyataan

- i. Maklumat terperingkat, sulit, sensitif, data peribadi dan dokumen rasmi PSUK Selangor dilarang dimasukkan ke dalam platform AI awam tanpa kelulusan rasmi.
- ii. Penggunaan AI hendaklah mematuhi klasifikasi maklumat dan Arahan Keselamatan yang sedang berkuat kuasa.
- iii. Sebarang pemprosesan data menggunakan AI hendaklah memastikan:
 - a) Data diminimumkan
 - b) Data disanitasi
 - c) Data dienkripsi
 - d) Akses dikawal
 - e) Aktiviti direkodkan
- iv. Platform AI yang digunakan hendaklah mempunyai kawalan keselamatan yang bersesuaian termasuk:
 - a) Pengurusan identiti dan akses
 - b) Logging dan monitoring
 - c) Perlindungan data
 - d) Kawalan perkongsian data
 - e) Audit trail
- v. *Output* yang dijana oleh AI hendaklah disemak sebelum digunakan bagi mengelakkan penyebaran maklumat tidak tepat atau mengelirukan.

PERANAN

ICTSO, Pemilik Maklumat, Pentadbir Sistem ICT.



SEKSYEN 8

PENGURUSAN KESELAMATAN FIZIKAL

Physical Security Management

PENGURUSAN KESELAMATAN FIZIKAL

PHYSICAL SECURITY MANAGEMENT

8.1 (A.7.1) Perimeter Keselamatan Fizikal

(Physical Security Perimeters)

Objektif: Untuk mencegah akses fizikal tanpa kebenaran, kerosakan dan gangguan terhadap maklumat serta aset berkaitan organisasi.

8.1.1 Perimeter Keselamatan Fizikal

(Physical Security Parameter)

Pernyataan

Perimeter keselamatan fizikal yang jelas hendaklah diwujudkan bagi tujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal, melindungi premis dan aset PSUK dan PDT Selangor, individu dan persekitaran fizikal daripada ancaman, bahaya atau kemungkinan kerosakan.

PERANAN

BKP

8.2 (A.7.2) Kemasukan Fizikal

(Physical Entry)

Objektif: Untuk memastikan hanya akses fizikal yang dibenarkan sahaja diberikan kepada maklumat dan aset berkaitan organisasi.

8.2.1 Kawalan Kemasukan Fizikal

(Physical Entry Controls)

Pernyataan

- i. Kemasukan ke kawasan selamat hendaklah dikawal bagi memastikan hanya individu yang diberi kuasa dibenarkan masuk.
- ii. Prosedur hendaklah merangkumi kawalan berikut:
 - a) Pelawat dan pembekal atau pihak ketiga tidak dibenarkan memasuki kawasan selamat tanpa pengawasan; dan
 - b) Log akses fizikal (contohnya tarikh, masa masuk dan keluar serta tujuan lawatan) bagi pelawat dan pembekal atau pihak ketiga hendaklah direkodkan.

PERANAN

Warga SUK dan PDT Selangor, Pelawat, Pembekal, Pihak Ketiga.

8.2.2 Kawasan Penyerahan dan Pemunggahan (*Delivery and Unloading Area*)

Pernyataan

Perkara-perkara yang perlu dilakukan dalam memastikan kawasan penyerahan dan pemunggahan selamat adalah seperti yang berikut:

- i. Pintu masuk seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan; dan
- ii. PSUK Selangor hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.

PERANAN

BKP

8.3 (A.7.3) Keselamatan Pejabat, Bilik, dan Kemudahan

(Securing Offices, Rooms, and Facilities)

Objektif: Untuk mencegah akses fizikal tanpa kebenaran, kerosakan dan gangguan terhadap maklumat serta aset berkaitan di pejabat, bilik dan kemudahan.

8.3.1 Keselamatan Fizikal Pejabat, Bilik dan Kemudahan

(Physical Security of Offices, Rooms and Facilities)

Pernyataan

- i. Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan.
- ii. Perkara yang perlu dipatuhi adalah seperti yang berikut:
 - a) Proses bekerja di kawasan selamat hendaklah dibangunkan dan dilaksanakan;
 - b) Pengasingan lokasi-lokasi terperingkat daripada laluan akses awam;
 - c) Akses ke tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan CCTV dan pusat data hendaklah dihadkan kepada yang diberi kebenaran bertugas sahaja;
 - d) Pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital Kerajaan Negeri Selangor yang diberi akses ke ruang operasi ICT, pusat data atau *server room* dan bilik rangkaian hendaklah diiringi oleh wakil PSUK atau PDT Selangor sepanjang masa; dan
 - e) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi Arahan Keselamatan yang sedang berkuat kuasa.

PERANAN

Ketua Jabatan, Pentadbir Pusat Data, Warga SUK dan PDT Selangor, Pelawat, Pembekal, Pihak Ketiga.

8.4 (A.7.4) Pemantauan Keselamatan Fizikal

(Physical Security Monitoring)

Objektif : Untuk mengesan dan mencegah akses fizikal tanpa kebenaran.

Pernyataan

Perkara berikut perlu dipatuhi dalam pemantauan keselamatan fizikal:-

- i. Lokasi yang menempatkan sistem-sistem kritikal hendaklah direka bentuk dengan peralatan atau sistem kawalan keselamatan yang bersesuaian yang boleh memantau akses secara berterusan serta pergerakan warga atau pelawat ke lokasi tersebut bagi mengesan akses yang tidak dibenarkan.
- ii. Capaian kepada bangunan yang menempatkan sistem kritikal harus dipantau secara berterusan untuk mengesan capaian yang tidak dibenarkan atau tingkah laku yang mencurigakan.

PERANAN

BKP, Pentadbir Pusat Data.

8.5 (A.7.5) Melindungi Terhadap Ancaman Fizikal dan Alam Sekitar

(Protecting Against Physical and Environmental Threats)

Objektif: Untuk mencegah atau mengurangkan kesan kejadian yang berpunca daripada ancaman fizikal dan persekitaran.

Pernyataan

- i. Perlindungan fizikal terhadap bencana alam, kebakaran, banjir, letupan, kacau bilau, serangan berniat jahat atau kemalangan hendaklah dirancang dan dilaksanakan seperti dalam Garis Panduan Pengurusan Kesenambungan Perkhidmatan (PKP) Sektor Awam.

- ii. Perlindungan peralatan daripada ancaman fizikal dan persekitaran hendaklah mematuhi perkara berikut:
 - a) Peralatan ICT yang ditempatkan di *Server Room* atau Pusat Data hendaklah diletakkan di lokasi yang sesuai dan dilindungi daripada ancaman serta bahaya persekitaran (contohnya kebakaran, asap, banjir, habuk, gangguan bekalan elektrik) serta akses tanpa kebenaran (contohnya kecurian) bagi memastikan operasi berterusan; dan
 - b) Semua peralatan ICT hendaklah diselenggara mengikut selang servis dan spesifikasi yang disyorkan oleh pembekal.

PERANAN

BKP, Pentadbir Pusat Data.

8.6 (A.7.6) Bekerja di Kawasan Selamat

(Working in Secure Areas)

Objektif: Untuk melindungi maklumat dan aset berkaitan daripada kerosakan dan gangguan tanpa kebenaran oleh personel yang bekerja di kawasan tersebut.

Pernyataan

Perkara berikut perlu dipatuhi bagi memastikan bekerja di kawasan selamat:

- i. Langkah-langkah kawalan keselamatan semasa bekerja di kawasan terperingkat hendaklah dirangka dan dilaksanakan. Kawasan terperingkat ditakrifkan sebagai kawasan yang dihadkan akses kemasukan kepada warga yang tertentu sahaja bagi melindungi aset ICT yang ditempatkan di lokasi tersebut.
- ii. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam.

PERANAN

Ketua Jabatan, Pentadbir Pusat Data, Warga SUK dan PDT Selangor .

8.7 (A.7.7) Meja Kosong dan Skrin Kosong

(*Clear Desk dan Clear Screen*)

Objektif: Untuk mengurangkan risiko akses tanpa kebenaran, kehilangan atau kerosakan maklumat di atas meja, skrin dan lokasi lain yang mudah diakses semasa dan selepas waktu bekerja.

Pernyataan

- i. Polisi Meja Kosong dan Skrin Kosong bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada di atas meja pengguna, pada paparan skrin komputer, mesin pencetak, mesin faksimili atau mesin pengimbas apabila pengguna tidak berada di tempatnya.
- ii. Polisi ini merangkumi aspek-aspek berikut:
 - a) Penggunaan fungsi kata laluan penyelamat skrin (*screen saver password*) atau log keluar apabila meninggalkan komputer;
 - b) Pengaktifan fungsi mod senyap;
 - c) Penyimpanan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci;
 - d) Semua dokumen hendaklah diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat;
 - e) Pengawalan e-mel masuk dan keluar;
 - f) Kawalan penggunaan mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital;
 - g) Penetapan dan hebahan peraturan serta panduan berkaitan konfigurasi mesej timbul (*pop-up message*) di skrin (contohnya mematikan *pop-up* e-mel dan mesej baharu semasa pembentangan, perkongsian skrin atau di kawasan awam); dan

- h) Memadamkan maklumat sensitif atau kritikal pada papan putih dan jenis paparan lain apabila tidak diperlukan lagi

PERANAN

Ketua Jabatan, Warga SUK dan PDT Selangor.

8.8 (A.7.8) Penempatan dan Perlindungan Peralatan *(Equipment Siting and Protection)*

Objektif: Untuk mengurangkan risiko daripada ancaman fizikal dan persekitaran serta akses tanpa kebenaran dan kerosakan.

Pernyataan

Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan.

PERANAN

BPSM, Warga SUK dan PDT Selangor.

8.9 (A.7.9) Keselamatan Aset Di Luar Premis *(Security of Assets Off-Premises)*

Objektif: Untuk mencegah kehilangan, kerosakan, kecurian atau kompromi peranti di luar premis serta gangguan kepada operasi organisasi.

Pernyataan

- i. Aset-aset di luar premis hendaklah dikawal dengan rapi bagi mengelak risiko kehilangan, rosak atau kecurian.

ii. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

- a) Peralatan, maklumat atau perisian tidak boleh dibawa keluar dari premis tanpa kebenaran terlebih dahulu; dan
- b) Kawalan keselamatan hendaklah dilaksanakan ke atas aset di luar premis dengan mengambil kira risiko yang berbeza apabila bekerja di luar premis PSUK dan PDT Selangor.

PERANAN

Ketua Jabatan, Pembekal dan Pihak Ketiga, Warga SUK dan PDT Selangor.

8.10 (A.7.11) Utiliti Sokongan

(Supporting Utilities)

Objektif: Untuk mencegah kehilangan, kerosakan atau kompromi maklumat dan aset berkaitan lain serta gangguan kepada operasi organisasi akibat kegagalan utiliti sokongan.

Pernyataan

Perkara yang perlu dipatuhi adalah seperti berikut:

- i. Peralatan hendaklah dilindungi daripada kegagalan bekalan kuasa dan gangguan lain akibat kegagalan utiliti sokongan;
- ii. Semua utiliti sokongan seperti bekalan elektrik, air, kumbahan, pemanasan atau pengudaraan dan penyaman udara hendaklah mencukupi untuk menyokong sistem yang berkaitan; dan
- iii. Semua utiliti sokongan hendaklah diselenggara secara berkala sekurang-kurangnya setahun sekali atau berdasarkan kontrak yang sedang berkuat kuasa.

PERANAN

BKP, Pegawai Aset, Pentadbir Aset.

8.11 (A.7.12) Keselamatan Kabel (Cabling Security)

Objektif: Untuk mencegah kehilangan, kerosakan, kecurian atau kompromi maklumat dan aset berkaitan lain serta gangguan kepada operasi organisasi yang berkaitan dengan pendawaian kuasa dan komunikasi.

Pernyataan

- i. Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan.
- ii. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi.
- iii. Langkah-langkah keselamatan yang perlu diambil ialah seperti yang berikut:
 - a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;
 - b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;
 - c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan pemintasan maklumat pada kabel; dan
 - d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui sesalur kabel bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.

PERANAN

Pentadbir Sistem ICT, Pegawai Aset, Pentadbir Aset.



SEKSYEN 9

PENGURUSAN KESELAMATAN RANGKAIAN

Network Security Management

PENGURUSAN KESELAMATAN RANGKAIAN

NETWORK SECURITY MANAGEMENT

9.1 (A.6.7) Kerja Jarak Jauh

(Remote Working)

Objektif : Untuk memastikan keselamatan maklumat apabila personel bekerja dari lokasi luar.

Pernyataan

- i. Langkah keselamatan hendaklah dilaksanakan bagi melindungi daripada risiko penggunaan kemudahan pengkomputeran mudah alih dan komunikasi. Polisi dan prosedur bagi memastikan penggunaan kemudahan pengkomputeran mudah alih secara selamat hendaklah diwujudkan dan dilaksanakan.
- ii. Warga yang bekerja jarak jauh hendaklah:
 - a) Memastikan keselamatan maklumat PSUK Selangor dipatuhi dan tidak disebarakan kepada pihak ketiga;
 - b) Memastikan arahan bekerja dari luar dipatuhi mengikut garis panduan yang ditetapkan;
 - c) Perlu mengambil kira keselamatan fizikal lokasi dan persekitaran tempat bekerja jarak jauh;
 - d) Memastikan keselamatan kawalan capaian bagi dokumen terperingkat pada peranti yang digunakan untuk bekerja jarak jauh;
 - e) Penggunaan capaian desktop maya perlu mengambil kira maklumat terperingkat, sensitiviti sistem dan aplikasi;

- f) Capaian maklumat jarak jauh hendaklah terhad kepada capaian rumah berbanding capaian awam; dan
- g) Menggunakan langkah-langkah keselamatan ke atas peranti yang digunakan bagi tujuan jarak jauh seperti *Antivirus*, *Firewall* dan *Malware Protection*.

PERANAN

Ketua Jabatan, Warga SUK & PDT Selangor.

9.2 (A.8.20) Keselamatan Rangkaian

(Network Security)

Objektif: Untuk melindungi maklumat dalam rangkaian dan kemudahan pemprosesan maklumat yang berkaitan daripada ancaman melalui rangkaian.

Pernyataan

- i. Infrastruktur rangkaian hendaklah dikawal dan diuruskan sebaik mungkin dalam infrastruktur rangkaian daripada sebarang ancaman demi melindungi ancaman kepada sistem dan aplikasi dalam rangkaian.
- ii. Rangkaian hendaklah dilindungi seperti berikut:
 - a) Rangkaian hendaklah diurus dan dikawal bagi melindungi maklumat dalam sistem dan aplikasi; dan
 - b) Akses kepada dokumentasi seni bina rangkaian PSUK dan PDT Selangor seperti rajah rangkaian, inventori infrastruktur, fail konfigurasi dan sebagainya hendaklah dihadkan hanya kepada pengguna yang diberi kuasa.

PERANAN

Pentadbir Rangkaian dan Keselamatan

9.3 (A.8.21) Keselamatan Perkhidmatan Rangkaian (Security of Network Services)

Objektif: Untuk memastikan keselamatan dalam penggunaan perkhidmatan rangkaian.

9.3.1 Pengasingan Kawalan Sempadan (Border Control Segregation)

Pernyataan

Memastikan pengasingan kawalan sempadan ke atas perkhidmatan rangkaian yang disediakan untuk meminimumkan risiko capaian tidak sah, ancaman atau pengubahsuaian yang tidak dibenarkan.

PERANAN

ICTSO

9.3.2 Pengurusan Perkhidmatan Rangkaian (Network Service Management)

Pernyataan

- i. Mekanisme keselamatan, tahap ketersediaan perkhidmatan dan keperluan pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan disediakan secara dalaman ataupun penyumberan luar.
- ii. Peraturan bagi penggunaan perkhidmatan rangkaian meliputi bagi perkara-perkara berikut:
 - a) Menggunakan teknologi keselamatan perkhidmatan rangkaian seperti pengesahan identiti, kawalan akses atau penggunaan enkripsi;
 - b) Memastikan peralatan rangkaian mematuhi polisi yang ditetapkan bagi menjamin keselamatan sambungan rangkaian;

- c) Memastikan kawalan akses kepada perkhidmatan rangkaian dan sistem aplikasi mengikut yang diluluskan;
- d) Memastikan trafik rangkaian dipantau dan dikawal oleh peralatan keselamatan;
- e) Memastikan pihak penyedia khidmat rangkaian mematuhi SLA yang telah dimeterai bagi mengelakkan ketersediaan rangkaian terjejas;
- f) Menggunakan peralatan *Web Content Filtering* bagi mengawal akses ke laman web yang tidak dibenarkan; dan
- g) Menyediakan dan mengawal penggunaan *Virtual Private Network (VPN)* dan rangkaian tanpa wayar (*wireless*) kepada pengguna yang diberi hak akses.

PERANAN

ICTSO, Pentadbir Sistem ICT.

9.4 (A.8.22) Pengasingan Rangkaian

(Segregation of Networks)

Objektif: Untuk membahagikan rangkaian kepada sempadan keselamatan dan mengawal aliran trafik berdasarkan keperluan perkhidmatan.

Pernyataan

Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian.

Pengasingan rangkaian hendaklah dilaksanakan seperti berikut:

- i. Perkhidmatan maklumat, pengguna dan sistem maklumat PSUK dan PDT Selangor hendaklah diasingkan dalam rangkaian menggunakan *Virtual LAN (VLAN)* dan dikawal di sempadan rangkaian menggunakan gerbang seperti tembok api (*firewall*) atau penghala penapisan;

- ii. Rangkaian tanpa wayar yang digunakan untuk penghantaran data hendaklah sentiasa dikonfigurasi dengan tembok api bagi menapis komunikasi dengan peranti jauh;
- iii. Semua sambungan LAN tanpa wayar hendaklah disahkan (*authenticated*) sebelum akses diberikan ke rangkaian dalaman PSUK dan PDT Selangor;
- iv. Titik capaian tanpa wayar (*Wireless Access Point* – WAP) hendaklah ditempatkan di kawasan fizikal yang selamat dalam premis PSUK dan PDT Selangor; dan
- v. Pengimbasan berkala hendaklah dijalankan bagi mengesan titik capaian tidak sah (*rogue access points*).

PERANAN

Pentadbir Keselamatan dan Rangkaian

9.5 (A.8.23) Penapisan Web

(*Web Filtering*)

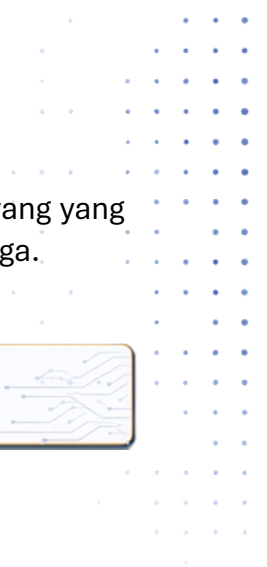
Objektif: Untuk melindungi sistem daripada dikompromi oleh perisian hasad serta menghalang akses kepada sumber laman sesawang yang tidak dibenarkan.

Pernyataan

Kawalan penyaringan laman sesawang perlu dilaksanakan bagi memastikan akses ke laman sesawang dilindungi dan menyekat akses ke laman sesawang yang tidak dibenarkan.

Sistem hendaklah dilindungi daripada di kompromi dan daripada akses kepada sumber laman sesawang yang tidak dibenarkan seperti berikut:

- i. PSUK Selangor hendaklah mengurangkan risiko warga mengakses laman sesawang yang mengandungi maklumat tidak sah atau yang diketahui mengandungi virus atau bahan *phishing*; dan

- 
- 
- ii. PSUK Selangor hendaklah mengenal pasti laman sesawang yang dibenarkan dan tidak dibenarkan untuk diakses oleh warga.

PERANAN

ICTSO, Pentadbir Keselamatan dan Rangkaian.





SEKSYEN 10

PENGURUSAN KESELAMATAN SISTEM DAN APLIKASI

*System and Application Security
Management*

PENGURUSAN KESELAMATAN SISTEM DAN APLIKASI

SYSTEM AND APPLICATION SECURITY MANAGEMENT

10.1 (A.8.4) Akses kepada Kod Sumber

(Access to Source Code)

Objektif: Untuk mencegah pengenalan fungsi tanpa kebenaran, mengelakkan perubahan yang tidak disengajakan atau berniat jahat, serta mengekalkan kerahsiaan harta intelek yang bernilai.

Pernyataan

Capaian kepada kod sumber hendaklah dihadkan bagi mengelakkan penambahan fungsi yang tidak dibenarkan, perubahan yang tidak disengajakan atau berniat jahat dan mengekalkan kerahsiaan harta intelek.

PERANAN

Pentadbir Sistem Aplikasi, Pengurus Projek, Pembekal, Pihak Ketiga.

10.2 (A.8.9) Pengurusan Konfigurasi

(Configuration Management)

Objektif: Untuk memastikan perkakasan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul mengikut konfigurasi keselamatan yang ditetapkan serta tidak diubah oleh perubahan yang tidak dibenarkan atau tidak tepat.

Pernyataan

- i. Pengurusan konfigurasi perlu dilaksanakan untuk memastikan perkakasan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul seiring dengan keperluan keselamatan dan memastikan konfigurasi tidak diubah tanpa kebenaran.
- ii. Perkara yang perlu dipatuhi ialah seperti yang berikut:
 - a) Melindungi capaian terhadap fail konfigurasi mengikut kawalan yang ditetapkan;
 - b) Merekod dan menyimpan sebarang perubahan konfigurasi dengan selamat; dan
 - c) Memantau konfigurasi dan menilai kawalan keselamatan.

PERANAN

Pentadbir Sistem ICT

10.3 (8.18) Penggunaan Program Utiliti yang Mempunyai Hak Istimewa (Use of Privileged Utility Programs)

Objektif: Untuk memastikan penggunaan program utiliti tidak menjejaskan kawalan keselamatan sistem dan aplikasi.

Pernyataan

- i. Penggunaan program utiliti yang boleh mengatasi (*overriding*) kawalan sistem dan aplikasi hendaklah dikawal dan dihadkan kepada pegawai yang dibenarkan sahaja.
- ii. Perkara yang perlu dipatuhi ialah seperti yang berikut:
 - a) Had penggunaan program utiliti kepada bilangan praktikal minimum pengguna yang dipercayai dan dibenarkan;
 - b) Penggunaan prosedur pengenalan, pengesahan dan kebenaran untuk program utiliti, termasuk pengenalan unik pengguna program utiliti;
 - c) Mentakrif dan mendokumentasikan tahap kebenaran untuk program utiliti;
 - d) Kebenaran untuk menggunakan program utiliti secara *ad hoc*;
 - e) Melaksanakan pengasingan tugas dengan menghadkan capaian pengguna yang mempunyai capaian kepada program utiliti;
 - f) Mengalih keluar atau melumpuhkan semua program utiliti yang tidak diperlukan;
 - g) Menghadkan ketersediaan program utiliti; dan
 - h) Pengelogan semua penggunaan program utiliti.

PERANAN

Pemilik Sistem, Pentadbir Sistem Aplikasi.

10.4 (8.24) Penggunaan Kriptografi

(Use of Cryptography)

Objektif: Untuk memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, keaslian dan integriti maklumat selaras dengan keperluan perkhidmatan serta keselamatan maklumat, dengan mengambil kira keperluan perundangan, statutori, kawal selia dan kontrak.

10.4.1 Polisi Penggunaan Kawalan Kriptografi

(Policy on The Use of Cryptographic Control)

Pernyataan

Kriptografi merangkumi kaedah-kaedah seperti yang berikut:

- i. **Penyulitan Data:** Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat penyulitan semasa dalam simpanan atau semasa sedang dipindahkan.
- ii. **Tandatangan Digital:** Tandatangan digital digunakan bagi memastikan maklumat digital tulen dan mempunyai integriti serta tidak boleh disangkal.

PERANAN

ICTSO, Pengurus ICT, Pemilik Maklumat, Pentadbir Sistem ICT, Warga PSUK dan PDT Selangor.

10.4.2 Pengurusan Kunci Awam

(Public Key Management)

Pernyataan

Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam/*Public Key Infrastructure* (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

Perkara berikut perlu dipatuhi:

- i. Semua kunci kriptografi yang dihasilkan bagi melindungi maklumat terperingkat adalah hak milik Kerajaan;
- ii. Kunci kriptografi mestilah diuruskan, diselia dan dilindungi dengan menggunakan kaedah yang ditetapkan dan hendaklah dirahsiakan;
- iii. Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebarang tindakan tanpa kebenaran sepanjang kitaran hayat kunci tersebut.

PERANAN

Warga SUK dan PDT Selangor.

10.5 (8.19) Pemasangan Perisian pada Sistem Operasi

(Installation of Software on Operational Systems)

Objektif: Untuk memastikan integriti sistem operasi serta mencegah eksploitasi kerentanan teknikal.

10.5.1 Pemasangan Perisian pada Sistem yang Beroperasi

(Installation of Software on Operational Systems)

Pernyataan

- i. Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi.
- ii. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti yang berikut:
 - a) Pelan sandaran hendaklah dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian;
 - b) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya;
 - c) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur; dilaksanakan dan diperaku berjaya;
 - d) Pengemaskinian perisian operasi hanya boleh dilaksanakan oleh pentadbir terlatih atas kebenaran pengurusan;
 - e) Memastikan bahawa hanya kod boleh laku (*executable code*) yang telah diluluskan dan tiada kod pembangunan atau penyusun (*compilers*) dipasang pada sistem operasi;
 - f) Menggunakan sistem kawalan konfigurasi untuk mengekalkan kawalan semua perisian operasi serta dokumentasi sistem; dan

- g) Mengarkibkan versi lama perisian, bersama-sama dengan semua maklumat dan parameter, prosedur, butiran konfigurasi dan perisian sokongan diperlukan sebagai langkah luar jangka (*contingency*), selagi perisian itu diperlukan untuk membaca atau memproses data yang diarkibkan.

PERANAN

Ketua Jabatan, Pentadbir Sistem ICT.

10.5.2 Sekatan ke atas Pemasangan Perisian

(Restriction on Software Installation)

Pernyataan

- i. Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan.
- ii. Perkara yang perlu dipatuhi adalah seperti yang berikut:
 - a) Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga, pihak luaran yang mempunyai urusan dengan perkhidmatan ICT PSUK Selangor.
 - b) Memasang dan menggunakan perisian yang tulen, berdaftar dan dilindungi di bawah undang-undang bertulis yang berkuat kuasa; dan
 - c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.

PERANAN

Warga SUK dan PDT Selangor, Pembekal, Pihak Ketiga.

10.6 (8.25) Kitar Hayat Pembangunan Selamat

(Secure Development Life Cycle)

Objektif: Untuk memastikan keselamatan maklumat direka bentuk dan dilaksanakan dalam kitar hayat pembangunan selamat bagi perisian dan sistem.

Pernyataan

Pembangunan selamat bagi perisian dan sistem hendaklah diwujudkan dan dilaksanakan seperti berikut:

- i. Pembangunan selamat hendaklah menjadi keperluan dalam membangunkan perkhidmatan, seni bina, perisian dan sistem yang selamat (iaitu keselamatan dalam kitar hayat pembangunan perisian);
- ii. Perubahan kepada sistem dalam kitar hayat pembangunan hendaklah dikawal menggunakan prosedur kawalan perubahan yang formal;
- iii. Apabila platform operasi diubah, aplikasi kritikal perkhidmatan hendaklah disemak, diuji dan dikaji semula secara berkala bagi memastikan tiada kesan negatif terhadap operasi atau keselamatan organisasi; dan
- iv. Pengubahsuaian kepada pakej perisian serta semua perubahan hendaklah dikawal dengan ketat.

PERANAN

Pengurus ICT, Pentadbir ICT, Pembekal, Pihak Ketiga.

10.7 (8.26) Keperluan Keselamatan Aplikasi (Application Security Requirements)

Objektif: Untuk memastikan semua keperluan keselamatan maklumat dikenal pasti dan ditangani semasa pembangunan atau pemerolehan aplikasi.

Pernyataan

Keperluan keselamatan aplikasi hendaklah mematuhi perkara berikut:

- i. Keperluan berkaitan keselamatan maklumat hendaklah dimasukkan dalam keperluan bagi sistem maklumat baharu atau penambahbaikan kepada sistem sedia ada;

- ii. Maklumat yang terlibat dalam perkhidmatan aplikasi yang melalui rangkaian awam hendaklah dilindungi daripada aktiviti penipuan, pertikaian kontrak serta pendedahan dan pengubahsuaian tanpa kebenaran; dan
- iii. Maklumat dalam transaksi perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak lengkap, salah hala (*misrouting*), pengubahan mesej tanpa kebenaran, pendedahan tanpa kebenaran, penduaan atau serangan ulangan (*replay*).

PERANAN

Pentadbir ICT, Pemilik Sistem.

10.8 (8.27) Prinsip Seni Bina dan Kejuruteraan Sistem Selamat

(Secure System Architecture and Engineering Principles)

Objektif: Untuk memastikan sistem maklumat direka bentuk, dilaksanakan dan dioperasi kan secara selamat dalam kitar hayat pembangunan.

Pernyataan

- i. Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat.
- ii. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) sektor awam yang terkini.
- iii. Prinsip seni bina dan kejuruteraan sistem hendaklah dilaksanakan seperti berikut:

- a) Keselamatan hendaklah direka bentuk merentasi semua lapisan seni bina (perkhidmatan, data, aplikasi dan teknologi) dengan mengimbangi keperluan keselamatan maklumat dan kebolehcapaian;
- b) Persekitaran pembangunan selamat bagi pembangunan dan integrasi sistem yang merangkumi keseluruhan kitar hayat pembangunan sistem hendaklah diwujudkan.

PERANAN

Pentadbir Sistem Aplikasi, Pembangun Sistem.

10.9 (A8.28) Pengekodan Selamat

(Secure Coding)

Objektif: Untuk memastikan perisian ditulis dengan selamat, dengan itu mengurangkan bilangan potensi keselamatan maklumat kelemahan dalam perisian.

Pernyataan

Prinsip pengekodan selamat hendaklah digunakan untuk pembangunan perisian dan perkara berikut perlu dipatuhi:

- i. Kawalan capaian kepada kod sumber atau atur cara program perlu dilaksanakan bagi mengelakkan kecurian, pengubahsuaian dan penghapusan tanpa kebenaran.
- ii. Proses pembangunan sistem hendaklah melalui kitaran ketat yang berfasa dengan memastikan kod sumber yang dihasilkan diuji dan kemudian diperkemaskan.
- iii. Kod sumber hendaklah dilindungi daripada capaian yang tidak dibenarkan dengan menggunakan kawalan akses dan kawalan versi.

- iv. Penyelenggaraan dan pengemaskinian versi perisian alat pembangun bersepadu (*Integrated Development Environment Tools*) hendaklah dilaksanakan secara berkala.

PERANAN

Pentadbir Sistem ICT, Pembangun Sistem, Pemilik Sistem.

10.10 (A.8.29) Ujian Keselamatan dalam Pembangunan dan Penerimaan

(Security Testing in Development and Acceptance)

Objektif: Untuk mengesahkan bahawa keperluan keselamatan maklumat dipenuhi apabila aplikasi atau kod dilaksanakan ke persekitaran pengeluaran.

Pernyataan

Ujian dalam pembangunan dan penerimaan hendaklah mematuhi perkara berikut:

- i. Ujian fungsi keselamatan hendaklah dilaksanakan semasa fasa pembangunan;
- ii. Program ujian penerimaan dan kriteria berkaitan hendaklah diwujudkan bagi sistem baharu, naik taraf dan versi baharu;
- iii. Persekitaran ujian dan operasi hendaklah diasingkan bagi mengurangkan risiko akses tanpa kebenaran atau perubahan kepada persekitaran operasi;
- iv. Kriteria penerimaan bagi sistem maklumat baharu, naik taraf dan versi baharu hendaklah ditetapkan, dan ujian yang bersesuaian hendaklah dilaksanakan sebelum penerimaan; dan
- v. Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan (*vulnerability scanner*).

PERANAN

ICTSO, Pentadbir Sistem ICT, Pemilik Sistem.

10.11 (8.30) Penyumberan Luar

(Outsourced Development)

Objektif: Untuk memastikan langkah keselamatan maklumat yang diperlukan oleh organisasi dilaksanakan dalam pembangunan sistem secara penyumberan luar.

Pernyataan

PSUK Selangor hendaklah menyelia dan memantau aktiviti pembangunan sistem secara penyumberan luar, termasuk:

- i. Pengaturan pelesenan, pemilikan kod dan hak harta intelek (IP);
- ii. Jaminan kualiti;
- iii. Pengurusan hak akses; dan
- iv. Ujian keselamatan.

PERANAN

Ketua Jabatan

10.12 (8.31) Pengasingan Persekitaran Pembangunan, Ujian dan Pengeluaran

(Separation of Development, Test, and Production Environments)

Objektif : Untuk melindungi persekitaran pengeluaran dan data daripada kompromi akibat aktiviti pembangunan dan ujian.

Pernyataan

Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi.

PERANAN

Pentadbir Sistem ICT, Pentadbir Pusat Data.

10.13 (8.32) Pengurusan Perubahan (Change Management)

Objektif: Untuk mengekalkan keselamatan maklumat semasa melaksanakan perubahan.

Pernyataan

Pengurusan perubahan hendaklah mematuhi perkara berikut:

- i. Perubahan dalam organisasi, proses perkhidmatan, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal menggunakan prosedur kawalan perubahan yang telah ditetapkan.
- ii. Sebarang perubahan terhadap model AI, algoritma atau integrasi AI hendaklah melalui proses pengurusan perubahan PSUK dan PDT Selangor.
- iii. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan.
- iv. Apabila platform operasi berubah, aplikasi penting atau kritikal hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan organisasi.
- v. Pengubahsuaian ke atas pakej perisian tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.

PERANAN

ICTSO, Ketua Jabatan, Pengurus ICT, Pentadbir Sistem ICT, Pemilik Sistem.



SEKSYEN 11

PENGURUSAN IDENTITI DAN AKSES

Identity Management

PENGURUSAN IDENTITI DAN AKSES

IDENTITY MANAGEMENT

11.1 (A.5.15) Kawalan Akses

(Access Control)

Objektif: Untuk memastikan akses yang dibenarkan dan untuk menghalang capaian yang tidak dibenarkan kepada maklumat dan lain-lain yang berkaitan aset.

Pernyataan

- i. Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza.
- ii. Peraturan kawalan didokumenkan capaian hendaklah diwujudkan, dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini setahun sekali atau mengikut keperluan semasa.
- iii. Perkara yang perlu dipatuhi adalah seperti yang berikut:
 - a) Keselamatan hendaklah direka bentuk merentasi semua lapisan seni bina (perkhidmatan, data, aplikasi dan teknologi) dengan mengimbangi keperluan keselamatan maklumat dan kebolehcapaian;
 - b) Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian;
 - c) Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa;
 - d) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;
 - e) Pengasingan kawalan capaian;
 - f) Kebenaran rasmi permintaan akses;
 - g) Keperluan semakan hak akses berkala;
 - h) Pembatalan hak akses;

- i) Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan
- j) Keistimewaan akses (*access privilege*).

PERANAN

ICTSO, Ketua Jabatan, Pentadbir Sistem ICT.

11.2 (A.5.16) Pengurusan Identiti (Identity Management)

Objektif: Untuk membolehkan pengenalpastian unik individu dan sistem yang mengakses maklumat serta aset berkaitan organisasi, dan seterusnya membolehkan pemberian hak akses yang bersesuaian.

Pernyataan

- i. Pengurusan Identiti adalah bagi memastikan identiti (ID) adalah unik bagi individu yang mengakses sistem, maklumat organisasi dan aset-aset lain yang berkaitan di samping menetapkan hak akses yang bersesuaian.
- ii. Proses pengurusan identiti perlu memastikan perkara berikut dipatuhi:
 - a) ID pengguna hendaklah unik bertanggungjawab ke atas akaun tersebut;
 - b) Memastikan ID pengguna yang diberikan kepada lebih dari seorang individu (identiti bersama) hanya dibenarkan jika ada keperluan dan tertakluk kepada kelulusan serta direkodkan;
 - c) Memastikan perkakasan yang memerlukan ID pengguna mendapat kelulusan serta pengawasan berterusan;
 - d) Membatalkan, menamatkan dan menukar akaun pengguna atas sebab berikut:
 - 1. Bertukar bidang tugas kerja;
 - 2. Bertukar ke agensi lain;
 - 3. Bersara; atau
 - 4. Ditamatkan perkhidmatan.

- e) Akaun tunggal hanya dipetakan kepada entiti tunggal;
- f) Merekod semua aktiviti penting beserta maklumat pengesahan berkenaan penggunaan dan pengurusan akaun pengguna.

PERANAN

Warga SUK dan PDT Selangor, Pentadbir Sistem Aplikasi, Pentadbir Pusat Data, Pentadbir Keselamatan dan Rangkaian, Pentadbir Aset.

11.3 (A.8.2) Hak Akses Istimewa

(Privileged Access Rights)

Objektif: Untuk memastikan hanya pengguna yang dibenarkan, dengan komponen perisian dan perkhidmatan disediakan keistimewaan hak akses.

Pernyataan

- i. Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal bagi memastikan hanya pengguna yang dibenarkan, perisian dan perkhidmatan tertentu sahaja disediakan dengan hak akses istimewa.
- ii. Penetapan dan penggunaan hak akses perlu diberikan kawalan dan penyeliaan yang ketat mengikut keperluan skop tugas yang telah dikenal pasti berdasarkan prosedur yang berkuat kuasa.
- iii. ID pengguna dengan keistimewaan sistem khas hendaklah dikawal dan dihadkan kepada bilangan warga yang diberi kuasa sahaja. Ini termasuk ID yang digunakan untuk mentadbir fungsi pengubahsuaian kepada sistem pengoperasian, keselamatan dan log audit.

PERANAN

Ketua Jabatan, Pentadbir Sistem ICT, Warga SUK & PDT Selangor.

11.4 (A.5.17) Maklumat Pengesahan

(Authentication Information)

Objektif: Untuk memastikan pengesahan entiti dilaksanakan dengan betul serta mencegah kegagalan proses pengesahan.

11.4.1 Pengesahan Identiti

(Identity Authentication)

Pernyataan

- i. Peruntukan pengurusan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.
- ii. Pemilik sistem atau warga yang dilantik hendaklah mentakrif dan menyelenggara senarai kawalan akses (*Access Control List – ACL*) bagi aplikasi dan data.

PERANAN

Ketua Jabatan

11.4.2 Amalan Pengesahan

(Verification Practices)

Pernyataan

Warga perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti.

PERANAN

Warga SUK dan PDT Selangor.

11.5 (A.5.18) Hak Akses

(Access Rights)

Objektif: Untuk memastikan akses kepada maklumat dan aset berkaitan ditakrifkan serta dibenarkan berdasarkan keperluan perkhidmatan.

Pernyataan

- i. Hak akses kepada maklumat dan aset yang berkaitan hendaklah diperuntukkan, disediakan, disemak dan dikaji semula mengikut dasar atau peraturan atau garis panduan kawalan akses yang berkuatkuasa.
- ii. Proses pemberian dan penarikan hak akses fizikal dan logikal kepada identiti yang telah disahkan hendaklah merangkumi perkara berikut:
 - a) Hak akses pengguna hendaklah disemak secara berkala, dan kekerapan semakan hendaklah bergantung kepada tahap risiko. Sebagai contoh, kebenaran akses istimewa hendaklah disemak dengan lebih kerap berbanding akses pengguna biasa;
 - b) Hak akses warga kepada maklumat dan kemudahan pemprosesan maklumat hendaklah ditamatkan apabila berlaku penamatan pekerjaan, kontrak atau perjanjian, atau diselaraskan apabila berlaku perubahan; dan
 - c) Hak akses pengguna kepada aplikasi dan data hendaklah diwujudkan dan diselenggara berdasarkan permohonan emel yang diluluskan. Semua permohonan akses hendaklah menyatakan justifikasi permintaan dan diluluskan oleh pemilik sistem atau wakil yang diberi kuasa.

PERANAN

ICTSO, Ketua Jabatan, Pentadbir Sistem ICT, Pentadbir Pusat Data, Pentadbir Keselamatan dan Rangkaian.

11.6 (A.8.3) Sekatan Capaian Maklumat (Information access restriction)

Objektif: Untuk memastikan hanya akses yang dibenarkan diberikan serta mencegah akses tanpa kebenaran kepada maklumat dan aset berkaitan.

Pernyataan

Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian merangkumi perkara berikut:

- i. Tidak membenarkan pengguna yang tidak berdaftar mengakses maklumat sensitif.
- ii. Menyediakan mekanisme konfigurasi untuk mengawal capaian kepada maklumat dalam sistem, aplikasi dan perkhidmatan;
- iii. Mengawal data yang boleh diakses oleh pengguna tertentu;
- iv. Mengawal identiti atau kumpulan identiti yang mempunyai akses seperti membaca, menulis, memadam dan melaksanakan (*execute*); dan
- v. menyediakan kawalan capaian fizikal atau logikal untuk mengasingkan aplikasi sensitif, data aplikasi atau sistem.

PERANAN

Ketua Jabatan, Pemilik Sistem, Pentadbir Sistem ICT.

11.7 (A.8.5) Pengesahan Selamat (Secure Authentication)

Objektif : Untuk memastikan pengguna atau entiti disahkan secara selamat apabila akses kepada sistem, aplikasi dan perkhidmatan diberikan.

Pernyataan

Pengesahan selamat diimplementasi bagi memastikan pengguna disahkan secara selamat sebelum mencapai akses ke sistem, aplikasi

dan perkhidmatan. Capaian aplikasi sistem perlu mempunyai kaedah pengesanan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang akses yang tidak dibenarkan.

PERANAN

Ketua Jabatan, Pentadbir Sistem ICT.



SEKSYEN 12

PENGURUSAN ANCAMAN DAN KERENTANAN

*Threat and Vulnerability
Management*

PENGURUSAN ANCAMAN DAN KERENTANAN

THREAT AND VULNERABILITY MANAGEMENT

12.1 (A.5.7) Perisikan Ancaman

(Threat Intelligence)

Objektif: Untuk menyediakan kesedaran terhadap persekitaran ancaman organisasi supaya tindakan mitigasi yang bersesuaian dapat diambil.

Pernyataan

Maklumat berkaitan ancaman keselamatan maklumat yang berpotensi atau memberi ancaman kepada fungsi PSUK Selangor perlu diperoleh dan dianalisis untuk menghasilkan maklumat perisikan berkaitan ancaman.

PERANAN

CSIRT, Pemilik Sistem.

12.2 (A.8.8) Pengurusan Kerentanan Teknikal

(Management of Technical Vulnerabilities)

Objektif : Untuk mencegah eksploitasi terhadap kerentanan teknikal.

Pernyataan

- i. Maklumat berkaitan kerentanan teknikal sistem maklumat yang digunakan hendaklah disemak secara berkala bagi melindungi sistem maklumat, perisian, dan infrastruktur teknikal daripada ancaman dan serangan yang berkaitan dengan kerentanan.
- ii. Kawalan terhadap keterdedahan teknikal perlu dilaksanakan untuk melindungi sistem maklumat, perisian, dan infrastruktur teknikal organisasi daripada ancaman dan serangan yang berkaitan dengan kerentanan.

iii. Perkara yang perlu dipatuhi ialah seperti yang berikut:

- a) Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;
- b) Mengenal pasti, menilai dan menganalisis tahap risiko kerentanan yang wujud dalam sistem, perisian, dan rangkaian PSUK Selangor;
- c) Melaksanakan tindakan penambahbaikan untuk mengatasi kerentanan yang telah dikenal pasti, termasuk melaksanakan penambahbaikan keselamatan dan konfigurasi semula;
- d) Memantau sistem dan perisian secara berterusan untuk mengenal pasti kerentanan yang mungkin muncul dalam masa sebenar; dan
- e) Melaksanakan dan memastikan amalan terbaik dalam keselamatan teknikal dan pengurusan kerentanan.

PERANAN

CSIRT, Pengurus ICT, Pemilik Sistem, Pentadbir Sistem ICT.



SEKSYEN 13

PENGURUSAN PERISTWA KESELAMATAN SIBER

*Cyber Security Event
Management*

PENGURUSAN PERISTIWA KESELAMATAN SIBER

CYBER SECURITY EVENT MANAGEMENT

13.1 (A.5.24) Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Maklumat

(Information Security Incident Management Planning and Preparation)

Objektif: Untuk memastikan tindak balas yang cepat, berkesan, konsisten dan teratur terhadap insiden keselamatan maklumat atau siber, termasuk komunikasi berkaitan peristiwa keselamatan maklumat atau siber.

13.1.1 Tanggungjawab dan Prosedur

(Responsibilities and Procedure)

Pernyataan

- i. Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat dengan mentakrif, mewujudkan dan menyampaikan proses pengurusan insiden keselamatan maklumat dan tanggungjawab.
- ii. Pengurusan insiden siber di PSUK dan PDT Selangor adalah berdasarkan Prosedur Operasi Standard Pengurusan dan Pengendalian Insiden Keselamatan Siber yang sedang berkuat kuasa.
- iii. Perkara yang perlu dipatuhi adalah seperti yang berikut:
 - a) Memberikan kesedaran berkaitan Prosedur Operasi Standard Pengurusan dan Pengendalian Insiden Keselamatan Siber dan hebahan kepada warga sekiranya ada perubahan; dan

- b) Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.

PERANAN

CSIRT, ICTSO, Pengarah Bahagian dan Pemilik Projek/Sistem Aplikasi.

13.1.12 Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Siber

(Cyber Security Incident Management Planning and Preparation)

Pernyataan

Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat atau siber, termasuk komunikasi tentang kejadian, kerentanan dan kelemahan keselamatan.

PERANAN

ICTSO, CSIRT.

13.2 (A.5.25) Penilaian dan Keputusan mengenai Peristiwa Keselamatan Maklumat

(Assessment and Decision on Information Security Events)

Objektif: Untuk memastikan pengelasan dan keutamaan penilaian dan keputusan bagi keselamatan maklumat atau keselamatan siber dilaksanakan secara berkesan.

Pernyataan

Penilaian dan keputusan mengenai kejadian keselamatan maklumat atau keselamatan siber mestilah mengikut perkara berikut:

- i. Kejadian keselamatan maklumat atau keselamatan siber hendaklah dinilai dan ditentukan sama ada ia perlu diklasifikasikan sebagai insiden keselamatan maklumat;
- ii. Hasil penilaian dan keputusan hendaklah direkodkan secara terperinci bagi tujuan rujukan dan pengesahan pada masa hadapan; dan
- iii. PSUK Selangor hendaklah menetapkan serta melaksanakan prosedur dan untuk mengenal pasti, mengumpul, memperoleh dan memelihara maklumat yang boleh dijadikan sebagai bahan bukti.

PERANAN

ICTSO, Pemilik Sistem CSIRT.

13.3 (A.5.26) Tindak Balas Terhadap Insiden Keselamatan Maklumat (*Respons to Information Security Incidents*)

Objektif: Untuk mengurangkan kebarangkalian atau impak insiden pada masa hadapan.

Pernyataan

- i. Insiden keselamatan maklumat atau keselamatan siber hendaklah ditangani menurut prosedur yang didokumenkan.
- ii. Tindak balas terhadap insiden keselamatan siber atau maklumat adalah berdasarkan pekeliling, garis panduan, undang-undang yang sedang berkuat kuasa.
- iii. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut:
 - a) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku;
 - b) Menjalankan forensik digital sekiranya perlu;

- c) Menghubungi pihak yang berkenaan dengan secepat mungkin;
- d) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti;
- e) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;
- f) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;
- g) Menyediakan tindakan pemulihan segera;
- h) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.
- i) Sebaik sahaja insiden itu berjaya ditangani, ia hendaklah ditutup secara rasmi dan direkodkan;
- j) Melaksanakan analisis pasca-kejadian untuk mengenal pasti punca asal dan didokumentasikan mengikut prosedur yang ditakrifkan; dan
- k) Mengenal pasti dan mengurus kelemahan dan kelemahan keselamatan maklumat termasuk yang berkaitan dengan kawalan yang telah menyebabkan, menyumbang kepada atau gagal untuk menghalang kejadian itu.

PERANAN

ICTSO, CSIRT, Pemilik Sistem, Pemilik Maklumat.

13.4 (A.5.27) Belajar daripada Insiden Keselamatan Maklumat

(Learning from Information Security Incidents)

Objektif: Untuk mengurangkan kebarangkalian atau impak insiden pada masa hadapan.

Pernyataan

- i. Pengetahuan yang diperoleh daripada penganalisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya.

- ii. Setiap insiden keselamatan maklumat atau keselamatan siber hendaklah direkodkan.
- iii. Penilaian terhadap insiden tersebut perlu dilaksanakan bagi memastikan keberkesanan kawalan keselamatan yang telah dilaksanakan serta mengenal pasti keperluan penambahbaikan.
- iv. Maklumat yang diperolehi daripada penilaian insiden hendaklah digunakan untuk:
 - a) Mempertingkatkan pelan pengurusan insiden termasuk senario dan prosedur insiden;
 - b) Mengenal pasti insiden berulang atau serius dan puncanya untuk mengemas kini penilaian risiko keselamatan maklumat atau keselamatan siber PSUK Selangor dan menentukan serta melaksanakan kawalan tambahan yang diperlukan untuk mengurangkan kemungkinan atau akibat kejadian serupa pada masa hadapan. Mekanisme untuk membolehkan itu termasuk mengumpul, mengukur dan memantau maklumat tentang jenis insiden, kekerapan insiden serta kos yang terlibat; dan
 - c) Meningkatkan kesedaran dan latihan pengguna dengan memberikan contoh tentang perkara yang boleh berlaku, cara bertindak balas terhadap insiden tersebut dan cara mengelak pada masa hadapan.

PERANAN

CSIRT, Pemilik Sistem, Pemilik Maklumat.

13.5 (A.5.28) Pengumpulan Bukti (Collection of Evidence)

Objektif : Untuk memastikan pengurusan bukti yang konsisten dan berkesan berkaitan insiden keselamatan maklumat atau keselamatan siber bagi tujuan tindakan tatatertib dan perundangan.

Pernyataan

Mewujudkan dan melaksanakan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliharaan artifak yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.

PERANAN

CSIRT, Pemilik Sistem, Pemilik Maklumat.

13.6 (A.6.8) Pelaporan Insiden Keselamatan Maklumat (Information Security Event Reporting)

Objektif: Untuk menyokong pelaporan insiden keselamatan maklumat atau keselamatan siber yang tepat pada masanya, konsisten dan berkesan oleh personel.

13.6.1 Pelaporan Insiden Keselamatan Siber atau Maklumat (Reporting Cyber or Information Security Events)

Pernyataan

- i. Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan bagi memastikan pengendalian insiden keselamatan siber dilaksanakan secara teratur.
- ii. Tindak balas terhadap setiap insiden hendaklah dilaksanakan dengan cepat dan berkesan berdasarkan pekeliling atau prosedur pengendalian insiden yang sedang berkuat kuasa.
- iii. Perkara yang perlu dipatuhi ialah seperti yang berikut:

- a) Menentukan mekanisme untuk melaporkan sebarang insiden melalui saluran dan dalam tempoh masa yang ditentukan;
 - b) Memberi kesedaran berkaitan prosedur pengendalian insiden dan hebahan kepada warga sekiranya terdapat perubahan; dan
 - c) Memastikan ahli jawatankuasa CSIRT dan Pemilik Sistem yang mengurus insiden siber mempunyai kompetensi yang diperlukan.
- iv. Insiden keselamatan maklumat atau keselamatan siber hendaklah dilaporkan kepada CSIRT berdasarkan prosedur pengendalian insiden yang berkuat kuasa.

PERANAN

ICTSO, Ketua Jabatan, CSIRT, Pemilik Sistem, Pentadbir Sistem ICT.

13.6.2 Pelaporan Kelemahan Keselamatan Maklumat

(Reporting Security Weaknesses)

Pernyataan

- i. Pentadbir Sistem hendaklah mengemukakan laporan pengurusan kerentanan teknikal (SPA, WASA, VAPT) kepada CSIRT yang melibatkan perkara berikut:-
 - a) Melibatkan aset-aset kritikal yang dikategorikan di bawah NCII; dan
 - b) Melaporkan kerentanan aset kritikal NCII yang tidak dapat diperbaiki atau diatasi berdasarkan laporan kerentanan teknikal.

- ii. Warga serta pembekal dan pihak ketiga yang menggunakan sistem dan perkhidmatan maklumat, hendaklah melaporkan sebarang kelemahan keselamatan maklumat yang diperhatikan atau disyaki dalam sistem atau perkhidmatan.

PERANAN

CSIRT, Pentadbir Sistem ICT, Pembekal, Pihak Ketiga, Warga SUK & PDT Selangor.

13.7 (A. 8.15) Pengelogan

(Logging)

Objektif: Untuk merekod peristiwa, menjana bukti, memastikan integriti maklumat log, mencegah akses tanpa kebenaran, mengenal pasti peristiwa keselamatan maklumat yang boleh membawa kepada insiden, serta menyokong siasatan.

Pernyataan

Log yang merekod aktiviti, pengecualian, ralat dan peristiwa berkaitan hendaklah dijana, disimpan, dilindungi dan dianalisis seperti berikut:

- i. Kemudahan log dan maklumat log hendaklah dilindungi daripada pengubahsuaian serta akses tanpa kebenaran;
- ii. Log audit yang mengandungi semua maklumat berkaitan hendaklah disimpan, terutamanya bagi perubahan kepada program operasi;
- iii. Aktiviti pentadbir sistem dan pengguna hendaklah direkodkan, dan semakan hendaklah dilaksanakan bagi memastikan akauntabiliti pengguna; dan
- iv. Maklumat log hendaklah dilindungi daripada perubahan dan akses tanpa izin.

PERANAN

Pentadbir Sistem ICT

13.8 (A.8.16) Pemantauan Aktiviti (Monitoring Activities)

Objektif: Untuk mengesan tingkah laku luar biasa (*anomalous behaviour*) dan potensi insiden keselamatan maklumat.

Pernyataan

- i. Rangkaian, sistem dan aplikasi hendaklah dipantau dan tindakan sewajarnya diambil untuk menilai kemungkinan insiden keselamatan maklumat.
- ii. PSUK Selangor perlu memantau untuk mengesan tingkah laku tidak normal (anomali) dan kemungkinan berlaku insiden keselamatan maklumat.
- iii. Pemantauan aktiviti perlu dilakukan seperti berikut:
 - a) Alat pemantauan automatik hendaklah dipasang bagi merekod, memantau dan mengesan sebarang aktiviti serta pelanggaran keselamatan yang melibatkan data pengeluaran (*production*) yang kritikal dan sensitif.
 - b) Alat tersebut hendaklah diluluskan dan diuji secara menyeluruh sebelum dilaksanakan.

PERANAN

Pentadbir Sistem ICT

13.9 (A.8.17) Penyegerakan Masa (Clock Synchronization)

Objektif: Untuk membolehkan korelasi dan analisis peristiwa berkaitan keselamatan serta data yang direkodkan, dan menyokong siasatan insiden keselamatan maklumat.

Pernyataan

Jam sistem (contohnya jam masa nyata dalam komputer atau peranti komunikasi) hendaklah disegerakkan merentasi rangkaian kawasan setempat (LAN).

PERANAN

Pentadbir Sistem ICT



SEKSYEN 14

PENGURUSAN KESINAMBUNGAN

Continuity Management

PENGURUSAN KESINAMBUNGAN

CONTINUITY MANAGEMENT

14.1 (A.5.29) Keselamatan Maklumat Semasa Gangguan

(Information Security During Disruption)

Objektif: Untuk melindungi maklumat dan aset berkaitan semasa gangguan.

Pernyataan

Maklumat dan aset semasa gangguan hendaklah dilindungi seperti berikut:

- i. Prosedur dan tanggungjawab hendaklah diwujudkan bagi memastikan tindak balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat atau keselamatan siber.
- ii. Kesenambungan keselamatan maklumat atau keselamatan siber hendaklah dimasukkan dalam pengurusan kesinambungan perkhidmatan.

PERANAN

CDO, ICTSO, Ketua Jabatan, CSIRT, Pasukan PKP.

14.2 (A.5.30) Kesiediaan ICT untuk Kesiambungan Perkhidmatan (ICT Readiness for Business Continuity)

Objektif: Untuk memastikan ketersediaan maklumat dan aset berkaitan organisasi semasa gangguan.

14.2.1 Kesiambungan Keselamatan Maklumat (Information Security Continuity)

Pernyataan

Pelan Pemulihan Bencana (*Disaster Recovery Plan – DRP*) hendaklah dibangunkan dan di selenggara bagi menyokong kesiambungan perkhidmatan di seluruh organisasi, dengan mengambil kira keperluan keselamatan maklumat.

PERANAN

CDO, ICTSO, Koordinator PKP, Pasukan Pemulihan Bencana ICT, CSIRT.

14.2.2 Perancangan Kesiambungan Keselamatan Maklumat (Planning Information Security Continuity)

Pernyataan

- i. PSUK Selangor hendaklah mengenal pasti keperluan keselamatan maklumat dan keselamatan siber bagi memastikan kesiambungan operasi dalam situasi kecemasan. Situasi tersebut termasuk krisis, bencana atau insiden lain yang boleh menjejaskan penyampaian perkhidmatan dan operasi organisasi.
- ii. Perancangan kesiambungan hendaklah mengambil kira isu dalaman dan luaran yang berkaitan serta risiko yang boleh memberi kesan terhadap sistem penyampaian perkhidmatan, fungsi kritikal organisasi, aset maklumat dan perkhidmatan ICT.

PERANAN

CDO, ICTSO, Ketua Jabatan, Jawatankuasa Pemandu PKP, Pasukan PKP, CSIRT.

14.2.3 Pengurusan Kesenambungan Perkhidmatan dan Keselamatan Maklumat

(Business Continuity and Information Security Management)

Pernyataan

PSUK Selangor hendaklah merancang, mendokumen, melaksana, menyelenggara dan menguji PKP berdasarkan objektif kesinambungan perkhidmatan dan keperluan kesinambungan ICT.

PERANAN

Jawatankuasa Pemandu, CSIRT, Pasukan PKP.

14.2.4 Menentukan, Mengkaji Semula dan Menilai Kesenambungan Keselamatan Maklumat atau Keselamatan Siber

(Verify, Review and Evaluate Information Security or Cyber Security Continuity)

Pernyataan

- i. PSUK Selangor hendaklah menguji dan mengesahkan kawalan Pengurusan Kesenambungan Perkhidmatan bagi keselamatan maklumat dan keselamatan siber yang telah diwujudkan.
- ii. Ujian dan pengesahan tersebut hendaklah dilaksanakan secara berkala bagi memastikan kawalan berkenaan kekal berkesan serta mampu menyokong kesinambungan operasi semasa berlakunya gangguan atau kegagalan pengoperasian.
- iii. PSUK Selangor hendaklah mengenal pasti dan memilih strategi kesinambungan ICT yang menyeluruh meliputi sebelum, semasa dan selepas kegagalan pengoperasian.

iv. PSUK Selangor hendaklah memastikan bahawa:

- a) Struktur yang mencukupi disediakan untuk menyediakan, mengurangkan dan bertindak balas terhadap gangguan yang disokong oleh kakitangan yang mempunyai tanggungjawab, kuasa dan kecekapan yang diperlukan;
- b) Pelan Pemulihan Bencana ICT perlu dinilai melalui latihan dan ujian secara kerap dan diluluskan oleh pihak pengurusan;
- c) Pelan Pemulihan Bencana ICT perlu menyatakan maklumat kesinambungan ICT berikut:
 - 1. Spesifikasi prestasi dan kapasiti untuk memenuhi keperluan dan objektif kesinambungan perkhidmatan seperti yang dinyatakan dalam BIA;
 - 2. *Maximum Tolerable Downtime* bagi setiap perkhidmatan ICT yang kritikal iaitu had tempoh gangguan yang boleh diterima.
 - 3. Objektif Masa Pemulihan (*RTO*) bagi setiap perkhidmatan ICT kritikal dan prosedur untuk memulihkan komponen tersebut; dan
 - 4. Objektif Titik Pemulihan (*RPO*) bagi perkhidmatan ICT yang kritikal ICT yang ditakrifkan sebagai jumlah maksimum kehilangan data yang boleh diterima berdasarkan masa.

PERANAN

CDO, ICTSO, CSIRT, Koordinator PKP, Pasukan Pemulihan Bencana ICT, Warga PSUK & PDT Selangor.

14.3 (A.8.6) Pengurusan Kapasiti

(Capacity Management)

Objektif: Untuk memastikan kapasiti yang mencukupi bagi kemudahan pemprosesan maklumat, sumber manusia, pejabat dan kemudahan lain.

Pernyataan

- i. Penggunaan sumber hendaklah dipantau dan disesuaikan.
- ii. Unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem sentiasa di tahap optimum.
- iii. Perkara yang perlu dipatuhi ialah seperti yang berikut:
 - a.) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang.
 - b) Kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.
 - c) Mempertimbangkan penggunaan pengkomputeran awan bagi pengurusan kapasiti yang berkesan, anjal (*elasticity*) dan boleh skala (*scalability*).

PERANAN

Pemilik Sistem, Pentadbir Sistem ICT.

14.4 (A.8.13) Sandaran Maklumat

(Information Backup)

Objektif: Untuk membolehkan pemulihan daripada kehilangan data atau sistem.

Pernyataan

Sandaran maklumat hendaklah dilindungi semasa proses pemulihan seperti berikut:

- i. Prosedur sandaran dan pemulihan yang mencukupi hendaklah didokumenkan bagi aplikasi dan data kritikal PSUK Selangor;
- ii. Pemilik sistem hendaklah bertanggungjawab menentukan keperluan sandaran berdasarkan klasifikasi dan sensitiviti data;
- iii. Maklumat kritikal hendaklah disandarkan di lokasi luar (*off-site*) yang berasingan daripada premis utama. Lokasi simpanan luar hendaklah mempunyai perlindungan fizikal dan persekitaran yang bersesuaian; dan
- iv. Media sandaran hendaklah diuji secara berkala bagi memastikan keupayaan memulihkan data yang disandarkan.

PERANAN

Pentadbir ICT, Pemilik Sistem.

14.5 (A.8.14) Kelewahan bagi Kemudahan Pemprosesan Maklumat

(Redundancy of Information Processing Facilities)

Objektif: Untuk memastikan operasi berterusan kemudahan pemprosesan maklumat.

Pernyataan

- i. PSUK Selangor hendaklah mengenal pasti keperluan bagi pelaksanaan mekanisme lewahan (*redundancy*) untuk kemudahan pemprosesan maklumat.
- ii. Mekanisme tersebut hendaklah direka bentuk dan dilaksanakan bagi memastikan kesinambungan perkhidmatan serta ketersediaan kemudahan pemprosesan maklumat.

PERANAN

Pentadbir Pusat Data, Pentadbir Sistem ICT.



SEKSYEN 15

UNDANG-UNDANG DAN PEMATUHAN

Regulation and Compliance

UNDANG-UNDANG DAN PEMATUHAN

REGULATION AND COMPLIANCE

15.1 (A.5.31) Pematuhan Terhadap Keperluan Perundangan dan Kontrak *(Legal, Statutory, Regulatory and Contractual Requirements)*

Objektif: Untuk memastikan pematuhan dengan keperluan undang-undang, berkanun, peraturan dan kontrak yang berkaitan dengan keselamatan maklumat.

Pernyataan

Perkara berikut perlu dilaksanakan:

- i. Meningkatkan dan memantapkan tahap keselamatan siber bagi mengelakkan pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.
- ii. Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga dan pembekal serta semua pihak yang terlibat dalam pembekalan perkhidmatan ICT. Keperluan perundangan yang perlu dipatuhi ialah seperti rujukan dokumen ini.
- iii. Penggunaan kriptografi hendaklah mematuhi keperluan perundangan, dasar dan pekeliling yang berkuat kuasa.
- iv. Penggunaan AI yang menyebabkan kebocoran data rasmi kerajaan boleh dikenakan tindakan tatatertib atau perundangan.

PERANAN

Warga SUK & PDT Selangor, Pembekal, Pihak Ketiga.

15.2 (A.5.32) Hak Harta Intelek

(Intellectual Property Rights)

Objektif: Untuk memastikan pematuhan terhadap keperluan perundangan, statutori, kawal selia dan kontrak berkaitan hak harta intelek serta penggunaan hak milik produk.

Pernyataan

Perkara berikut perlu dipatuhi:

- i. Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan dengan hak harta intelektual.
- ii. Melaksanakan kawalan terhadap keperluan pelesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.
- iii. Hak harta intelek bagi perisian, dokumentasi dan maklumat lain yang dihasilkan atau dibekalkan oleh warga serta pembekal untuk kepentingan PSUK dan PDT Selangor hendaklah menjadi milik PSUK Selangor .

PERANAN

Ketua Jabatan, Pemilik Sistem ICT, Pengurus Projek, Pembekal, Pihak Ketiga, Warga SUK & PDT Selangor.

15.3 (A.5.34) Privasi dan Perlindungan Maklumat Pengenalan Peribadi (*Privacy and Protection of Personally Identifiable Information - PII*)

Objektif: Untuk memastikan pematuhan terhadap keperluan perundangan, statutori, kawal selia dan kontrak berkaitan perlindungan maklumat pengenalan peribadi.

Pernyataan

Perkara tersebut perlu dipatuhi adalah seperti berikut:

- i. Maklumat pengenalan peribadi hendaklah dikendalikan selaras dengan 7 Prinsip Perlindungan Data Peribadi yang wajib dipatuhi di bawah seksyen 5(1) dalam Akta 709.
- ii. Organisasi hendaklah mengenal pasti dan memenuhi keperluan berkenaan pemeliharaan privasi dan perlindungan maklumat peribadi (PII) mengikut undang-undang dan peraturan yang berkenaan serta keperluan kontrak.

PERANAN

Ketua Jabatan

15.4 (A.5.36) Pematuhan kepada Polisi, Peraturan dan Piawaian Keselamatan Maklumat (*Compliance with Policies, Rules and Standards for Information Security*)

Objektif : Untuk memastikan keselamatan maklumat dilaksanakan dan dikendalikan selaras dengan polisi keselamatan maklumat organisasi, polisi khusus, peraturan dan piawaian yang ditetapkan.

15.4.1 Pematuhan Polisi dan Standard Keselamatan

(Compliance with Security Policies and Standards)

Pernyataan

Pematuhan terhadap pemprosesan maklumat dan prosedur dalam hendaklah disemak selaras dengan polisi, piawaian, dan keperluan keselamatan yang berkaitan.

PERANAN

CDO, ICTSO, Ketua Jabatan, Pemilik Sistem.

15.4.2 Kajian Semula Pematuhan Teknikal

(Technical Compliance Review)

Pernyataan

Kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung dalam polisi, piawaian dan keperluan komputer.

PERANAN

CDO, ICTSO, Pengurus ICT, Pemilik Sistem.

15.4.3 Pemantauan Audit Dalaman

Pernyataan

- i. Memastikan semua polisi, peraturan, akta dipatuhi dan dilaksanakan oleh semua peringkat proses perkhidmatan.
- ii. Pemantauan audit dalaman dilaksanakan sekali dalam tempoh 12 bulan (secara berkala) bagi memastikan semua jabatan dan bahagian mematuhi prosedur, dasar, peraturan dan undang-undang yang telah dikuatkuasakan.

PERANAN

ICTSO, Ketua Jabatan, Pentadbir Sistem ICT.



SEKSYEN 16

DOKUMEN STANDARD PROSEDUR OPERASI

Standard of Document Procedure

DOKUMEN STANDARD PROSEDUR OPERASI

STANDARD OF DOCUMENT PROCEDURE

16.1 (A.5.37) Prosedur Operasi yang Didokumenkan (Documented Operating Procedures)

Objektif: Untuk memastikan operasi kemudahan pemprosesan maklumat dilaksanakan dengan betul dan selamat.

16.1.1 Pengenalpastian proses kerja

Pernyataan

- i. PSUK dan PDT Selangor hendaklah mengenal pasti proses kerja yang perlu didokumenkan sebagai Prosedur Operasi Standard (SOP).
- ii. SOP tersebut hendaklah menjadi panduan kepada warga kerja dalam melaksanakan tugas yang melibatkan perkakasan dan sistem ICT.
- iii. Pelaksanaan SOP hendaklah memastikan proses kerja dilaksanakan secara teratur, konsisten, mengikut tatacara yang ditetapkan serta meminimumkan ralat.
- iv. Dokumentasi sistem (contohnya manual teknikal, panduan pentadbiran, manual pengguna, proses kebenaran dan sebagainya) hendaklah dilaksanakan dan dilindungi seperti berikut:

- a) Semua prosedur keselamatan siber yang diwujudkan, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal;
- b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan
- c) Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.

PERANAN

Pengurus ICT, Ketua Jabatan, Pentadbir Sistem ICT, Warga PSUK & PDT Selangor.

LAMPIRAN

Attachment



**SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER
PEJABAT SETIAUSAHA KERAJAAN NEGERI SELANGOR**

Nama (Huruf Besar) : _____

No . Kad Pengenalan : _____

Jawatan : _____

Bahagian /
Jabatan/Organisasi : _____

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber Pejabat Setiausaha Kerajaan Negeri Selangor.
2. Sekiranya saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan undang-undang boleh diambil ke atas diri saya.

Tandatangan :

Tarikh :

Pengesahan Pegawai Keselamatan ICT (ICTSO), PSUK Selangor

.....

Pegawai Keselamatan ICT (ICTSO)
b.p Setiausaha Kerajaan Negeri Selangor

Tarikh :

Cop Jabatan

Sekalung Penghargaan

TERIMA KASIH ATAS KOMITMEN, KEPIMPINAN DAN JASA DALAM
MEMPERKUKUH KESELAMATAN SIBER NEGERI SELANGOR



PENGHARGAAN

Pejabat Setiausaha Kerajaan Negeri Selangor merakamkan setinggi-tinggi penghargaan dan ucapan terima kasih kepada semua pihak yang telah menyumbangkan idea, pandangan, kepakaran serta komitmen dalam pembangunan Polisi Keselamatan Siber Pejabat Setiausaha Kerajaan Negeri Selangor Versi 1.0. Sumbangan dan kerjasama semua pihak telah memainkan peranan penting dalam memastikan polisi ini dibangunkan secara komprehensif dan memenuhi keperluan keselamatan siber organisasi.

YB DATO' SETIAUSAHA KERAJAAN NEGERI SELANGOR

YB DATO' DR. AHMAD FADZLI BIN AHMAD TAJUDDIN

MANTAN CDO

YBHG. DATO' YAZID BIN SAIRI

ICTSO PSUK SELANGOR

YBRS. TS. DR. ADI AZLAN BIN MOHD ALI

SETIAUSAHA BAHAGIAN PENGURUSAN MAKLUMAT

NOR RASHIDAH BINTI MOHD NOR

KETUA PENOLONG SETIAUSAHA KANAN

ABDUL WAHID BIN ABDUL MUTALIP

PENGURUS PROJEK

YBRS. TS. NURUL AZILAH BINTI JALIL

PENOLONG PENGURUS PROJEK

NAZIHAH BINTI ABD RAHMAN

URUSETIA

MOHD SYAKIR BIN MOHD ISHAK

MUHAMMAD FIRDAUS BIN ZULKIFLI

MUHAMMAD TAUFIQ BIN SULAIMAN

NOR AMIZA BINTI MOHD ZAKLI

BAHAGIAN PENGURUSAN MAKLUMAT

YBRS. TS. SHAZRINA BINTI ROSLAN
NURUL ELLIZA BINTI JASMIN
AZUA AKMA BINTI ABDULLAH SANI
NORDAHLIA BINTI ABDUL JALAL
MUHAMMAD HAFIZ BIN RAMLI
NURJIHAN BINTI ZULKARNAIN
ALLAHYARHAMAH TUAN ZAHARAH BINTI RAJA SOH
RAHAYU BINTI ABDUL RAHIM
ROSNAH BINTI MISKAN
MOHD HANIF BIN HAMDAN
AMIR HISHAM BIN DATO' HAJI AKALUDIN
NOOR WAHIDAH BINTI MAHAT
AMIRIZAM BIN MUSTAFA
MOHAMED SYAHID BIN MOHAMED YUNUS
MOHD ASRAF BIN ABDUL HALIM
NURUL SYUHADA BINTI ROSLAN
NORASHIKIN BINTI ABU BAKAR
ANIS NABILA BINTI ROSLI
SHAHINDAH FATINI BINTI MUDZAFAR SHAH
MUHAMAD NAIM BIN OSMAN
MUHAMMAD AZRI BIN MOHD JUSOH
SARATHE A/L RAJENDRAN
IZAN BINTI MOHAMAD TAIB
RASHIDAH BINTI KAMARUZAMAN
FATINUL KHASANAH BINTI AINI
NURSHAM AQMAL BIN SHAMSUL KAMAR
MUHAMMAD AMIN FAISAL BIN MUHAMAD NASIR

PEJABAT YB SETIAUSAHA KERAJAAN

AIDA SUHANA BINTI BARUDIN

BAHAGIAN PENGURUSAN SUMBER MANUSIA

MOHD RIZAL BIN MD ZAIN
MOHD ISHAM BIN ISMAIL

BAHAGIAN KORPORAT

MOHD FONTEDZA BIN MOHD RAWI

BAHAGIAN KHIDMAT PENGURUSAN

SITI NAWWAR BINTI NAJIB
LELY NADRAH BINTI SALLEH
IZAROHAYU BINTI ISHAK

UPEN – SEKSYEN MAKRO DAN PENSWASTAAN

KHAIRUL IZWAN BIN ABD AZIZ

UPEN – SEKSYEN SEKTORAL

MUHAMAD AZUWAN BIN ABDUL RAHMAN

UNIT MAJLIS MESYUARAT KERAJAAN NEGERI (MMKN)

RUHAIZAT BIN DAUD

PEJABAT DAERAH DAN TANAH PETALING

MUHAMMAD HAFIFI BIN SENARDI

PEJABAT DAERAH DAN TANAH KLANG

LILI BINTI IBRAHIM

PEJABAT DAERAH DAN TANAH GOMBAK

SITI NORLELA BINTI TASUKI@DASUKI

PEJABAT DAERAH DAN TANAH HULU LANGAT

MOHD ZULKIFLE BIN SALLEH

PEJABAT DAERAH DAN TANAH SEPANG

KAMALIAH BINTI MAHMUD

PEJABAT DAERAH DAN TANAH KUALA LANGAT

ARLINA BINTI MOHD AMIN

PEJABAT DAERAH DAN TANAH KUALA SELANGOR

RABIATUL ADAWIYAH BINTI ABDUL RAHAMAN

PEJABAT DAERAH DAN TANAH HULU SELANGOR

NOR HAZWANI BINTI MOHD RAZALI

PEJABAT DAERAH DAN TANAH SABAK BERNAM

MOHD SHARULNIZAM BIN RAKIBUN

PKS PSUK

SELANGOR

V1.0



BAHAGIAN PENGURUSAN MAKLUMAT
PEJABAT SETIAUSAHA
KERAJAAN NEGERI SELANGOR