
اونيۏرسيتي مليسيا ڤهڠ السلطان عبد الله
UNIVERSITI MALAYSIA PAHANG
AL-SULTAN ABDULLAH

# POLISI KESELAMATAN SIBER

**UNIVERSITI MALAYSIA PAHANG**
**AL-SULTAN ABDULLAH**
**(UMPSA)**

## SEJARAH DOKUMEN

| VERSI | KELULUSAN | TARIKH KUAT KUASA |
|---|---|---|
| 1.0 | Mesyuarat JPICT Bil. 2/2022 | 7 Jun 2022 |
| 2.0 | Mesyuarat JPICT Bil. 1/2025 | 3 Feb 2025 |

**ISI KANDUNGAN**

**TAKRIFAN**

Bagi maksud pemakaian Polisi Keselamatan Siber UMPSA ini:

| | | |
|---|---|---|
| (1) | Antivirus | Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM untuk sebarang kemungkinan adanya virus. |
| (2) | Aset Alih | Aset alih bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan. |
| (3) | Aset ICT | Aset ICT UMPSA merangkumi Maklumat, Aliran Data, Platform Aplikasi dan Perisian, Peranti Fizikal dan Sistem, Sistem Luaran serta Sumber Luaran. |
| (4) | BCP/PKP | *Business Continuity Planning*<br>Pelan Kesinambungan Perkhidmatan |
| (5) | Baki risiko | Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan. |
| (6) | *Bandwidth* | Jalur lebar<br>Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan. |
| (7) | Capaian *privilege* | Hak akses ke sesuatu maklumat/sistem mengikut fungsi yang berkenaan. |
| (8) | CCTV | *Closed-Circuit Television System*<br>Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal. |
| (9) | CIA | *Confidentiality, Integrity, Availability* |
| (10) | CIO | *Chief Information Office* |

| | | |
|---|---|---|
| | | Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan maklumat bagi menyokong arah tuju sesebuah organisasi. |
| (11) | *Clear Desk dan Clear Screen* | Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya. |
| (12) | *Contract for Service (CFS)* | Lain-lain lantikan (seperti Ikhtisas, Sambilan Post Doctoral, Visiting Lecturer).<br><br>CFS tidak mengguna pakai sebarang skim perkhidmatan, gred jawatan dan kadar gaji sebagaimana yang ditetapkan dalam Perkhidmatan Awam. Pelantikan CFS dipohon kepada Kementerian Kewangan bagi menetapkan syarat-syarat perkhidmatan yang tertentu. |
| (13) | *Contract of Service (COS)* | COS mengguna pakai skim perkhidmatan, gred dan kadar gaji sebagaimana yang ditetapkan di dalam Perkhidmatan Awam. |
| (14) | Data | Data merujuk kepada data mentah (*raw*), atau data yang tidak diproses. Ia adalah bentuk asas data, data yang tidak dianalisis atau diproses dengan apa-apa cara. Setelah data dianalisis, ia dianggap sebagai maklumat. |
| (15) | Data-dalam-simpanan<br><br>*(Data-at-rest*) | Merujuk kepada data yang disimpan di dalam destinasi sistem yang stabil. Data-dalam-simpanan sering kali diterjemahkan sebagai data yang tidak digunakan atau dipindahkan kepada peringkat akhir sistem seperti peranti telefon atau stesen kerja. |
| (16) | Data-dalam-pergerakan *(Data-in-motion)* | Merujuk kepada aliran data yang dipindahkan melalui pelbagai jenis rangkaian. Ia mewakili data yang sedang dialihkan atau dipindahkan. |

| | | |
|---|---|---|
| (17) | Data-dalam-penggunaan *(Data-in-use)* | Merujuk kepada data yang bukan hanya disimpan secara pasif di dalam destinasi yang stabil seperti pusat data, bahkan turut berfungsi melalui bahagian lain dalam seni bina IT. |
| (18) | *Denial of service* | Halangan / sekatan pemberian perkhidmatan. |
| (19) | *Defence-in-depth* | Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat. |
| (20) | Dokumen | Semua himpunan atau kumpulan bahan atau rekod yang disimpan dalam bentuk media cetak, salinan lembut *(soft copy),* elektronik, dalam talian, kertas lutsinar, risalah atau slaid. |
| (21) | *Downloading* | Aktiviti muat turun sesuatu perisian. |
| (22) | *Encryption* | Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah. |
| (23) | *Escrow* (eskrow) | Sebarang system yang membuat Salinan kunci penyulitan *(encryption)* supaya boleh dicapai oleh individu yang dibenarkan pada bila-bila masa. |
| (24) | *Failover test* | Satu teknik ujian yang mengesahkan keupayaan sistem untuk memperuntukkan sumber tambahan dan memindahkan operasi ke sistem sandaran semasa kegagalan *server*. |
| (25) | *Firewall* | Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya. |
| (26) | *Forgery* | Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat *(information theft/espionage) dan* penipuan *(hoaxes).* |

| | | |
|---|---|---|
| (27) | *Hard disk* | Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas. |
| (28) | *Hub* | Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan *(broadcast)* data yang diterima daripada sesuatu *port* kepada semua *port* yang lain. |
| (29) | ICT | *Information and Communication Technology*<br>Teknologi Maklumat dan Komunikasi |
| (30) | ICTSO | *ICT Security Officer* –<br>Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer. |
| (31) | Insiden Keselamatan | Musibah *(adverse event)* yang berlaku ke atas system maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut. |
| (32) | Internet | Internet adalah sistem rangkaian komunikasi global. Ia merangkumi infrastruktur perkakasan dan perisian yang menyediakan sambungan rangkaian global di antara komputer. Internet dalam skop UMPSA adalah servis rangkaian yang membolehkan pengguna mengakses sumber maklumat di seluruh dunia secara atas talian. |
| (33) | *Internet Gateway* | Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan. |
| (34) | ISDN | *Integrated Services Digital Network*<br>Menggunakan isyarat digital pada talian telefon analog yang sedia ada. |
| (35) | Intranet | Merujuk kepada jaringan rangkaian dalaman yang menghubungkan komputer di dalam sesebuah organisasi dan hanya boleh dicapai oleh staf atau |

| | | |
|---|---|---|
| | | mana-mana pihak yang dibenarkan. Intranet dalam skop UMPSA adalah servis rangkaian yang membolehkan pengguna mengakses sumber maklumat di dalam kampus UMPSA secara atas talian. |
| (36) | *Intrusion Detection System (IDS)* | Sistem Pengesan Pencerobohan<br>Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian. |
| (37) | *Intrusion Prevention System (IPS)* | Sistem Pencegah Pencerobohan 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 atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan. |
| (38) | ISMS | *Information Security Management System*<br>Sistem Pengurusan Keselamatan Maklumat |
| (39) | Keadaan Berisiko Tinggi | Dalam situasi yang mudah mendapat ancaman dari pihak luar atau apa-apa kemungkinan yang boleh menjejaskan kelancaran sistem. |
| (40) | Kemudahan ICT | Merujuk kepada perkakasan, peralatan, sistem dan perkhidmatan yang berkaitan teknologi maklumat dan telekomunikasi yang disediakan oleh UMPSA bagi tujuan pengurusan, pentadbiran, penyelidikan, pengajaran & pembelajaran serta operasi pengguna. |
| (41) | Kerentanan | Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan. |

| | | |
|---|---|---|
| (42) | Ketua Jabatan | Pegawai yang mengetuai sesuatu jabatan di UMPSA |
| (43) | Kod Sumber | Penyataan pengaturcaraan (programming statements) yang dibangunkan menggunakan bahasa dan arahan komputer, media elektronik seperti telefon pintar, komputer, laptop dan sebagainya. |
| (44) | Komunikasi digital | Komunikasi digital adalah merujuk kepada kaedah penyampaian maklumat atau infomasi di dalam bentuk eletroknik meliputi teks, mel elektronik, mel suara dan video dengan menggunakan teknologi digital atas talian melalui jaringan internet dengan penggunaan |
| (45) | Kriptografi | Kaedah untuk menukar data dan maklumat biasa *(standard format)* kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat. |
| (46) | LAN | *Local Area Network.*<br><br>Rangkaian komputer yang merangkumi kawasan fizikal yang kecil. LAN dalam skop UMPSA adalah rangkaian UMPSA Gambang atau rangkaian UMPSA Pekan. |
| (47) | *Lock* | Mengunci komputer. |
| (48) | *Logout* | *Log-out* komputer<br><br>Keluar daripada sesuatu sistem atau aplikasi komputer. |
| (49) | Maklumat Terperingkat | Maklumat terperingkat ialah dokumen yang mesti diberi perlindungan untuk kepentingan keselamatan dan yang bertanda dengan sesuatu peringkat keselamatan. Maklumat dalam dokumen terperingkat mesti diberi perlindungan keselamatan berdasarkan Arahan Keselamatan. |

| | | |
|---|---|---|
| (50) | *Malicious Code* | Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya. |
| (51) | Media | Peralatan atau perantara yang digunakan untuk menyimpan data dan maklumat seperti media USB, cakera padat, cakera keras, alat komunikasi mudahalih, komputer/laptop dan *public cloud storage*. |
| (52) | *Mobile Code* | *Mobile code* merupakan suatu perisian yang boleh dipindahkan di antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh Java Applet,<br><br>ActiveX dan sebagainya pada pelayar internet. |
| (53) | MODEM | MOdulator DEModulator<br><br>Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer. |
| (54) | *Network Time Protocol (NTP) Server* | NTP merupakan satu protokol untuk menyeragamkan masa dan tarikh antara pelayan di dalam UMPSA kepada satu (1) sumber iaitu berdasarkan kepada *"Malaysia Standard Time".* |
| (55) | *Outsource* | Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui. |
| (56) | Pasukan ERT | Pasukan Tindakan Kecemasan/*Emergency Response Team* (ERT). |
| (57) | Pegawai Aset | Pegawai yang menguruskan aset di PTJ masing-masing. |

| | | |
|---|---|---|
| (58) | Pegawai Penerima Aset | Pengawai penerima aset yang mengesahkan aset yang diterima adalah sama seperti spesifikasi perolehan yang dibuat. |
| (59) | Pegawai Pengelas | Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa. |
| (60) | Pelajar | Bermaksud seseorang pelajar berdaftar, selain pelajar di suatu institusi yang bersekutu dengan universiti, yang mengikuti kursus pengajian, pengajaran, latihan atau penyelidikan daripada apa-apa perihalan pada peringkat persediaan, praijazah, lepas ijazah atau lepas kedoktoran secara sepenuh masa atau sambilan dalam, oleh atau dari universiti, dan termasuklah pembelajaran jarak jauh, luar kampus dan pelajar pertukaran. |
| (61) | Pelaksana ICT | Staf ICT yang bertanggungjawab melaksanakan tugasan ICT yang berkaitan termasuklah pelaksana sistem aplikasi, pelaksana teknikal, pelaksana rangkaian, pelaksana laman web/portal, pelaksana e-mel serta pelaksana pusat data dan *Disaster Recovery Center (DRC)*. |
| (62) | Pemilik Aset ICT | Wakil-wakil PTJ yang memiliki dan menguruskan aset ICT UMPSA. |
| (63) | Pengguna | Staf dan pelajar UMPSA, Lembaga Pengarah UMPSA, ejen, pembekal, pakar runding dan lain-lain pihak yang berurusan dengan UMPSA. |
| (64) | Pengolahan risiko | Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksana berdasarkan hasil penilaian risiko. |
| (65) | Pengurus ICT | Gred F12-A ke atas di UMPSA/Staf yang mengetuai bahagian |

| | | |
|---|---|---|
| (66) | Pentadbir ICT | Ketua Seksyen / Ketua Unit di DiTec / Pegawai Penyelia / Ketua Teknikal ICT di UMPSA |
| (67) | Peranti mudah alih | Peranti mudah alih adalah sebarang peranti yang mudah dibawa. |
| (68) | Perisian aplikasi | Merujuk kepada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* atau pun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan. |
| (69) | Perisian yang diperaku | Perisian yang digunakan melalui perolehan UMPSA atau perisian tersebut memiliki lesen penggunaan. |
| (70) | Perkakasan teknologi | Perkakasan bagi kegunaan pembelajaran, pengajaran, pentadbiran dan penyelidikan seperti peralatan<br>pandang dengar dan yang berkaitan. |
| (71) | Perkhidmatan ICT | Kemudahan ICT bagi menyokong pengajaran dan pembelajaran, penyelidikan, pentadbiran dan pembangunan warga UMPSA. |
| (72) | Pihak ketiga | Pihak luar yang berurusan dengan pihak UMPSA. |
| (73) | PTJ | Pusat Tanggungjawab bermaksud semua jabatan, fakulti, pusat dan institut di UMPSA. |
| (74) | DiTec | Pusat Teknologi Digital |
| (75) | *Public cloud storage* | Pengkomputeran awan awam adalah tempat menyimpan dan mencapai data dan aplikasi dengan menggunakan Internet selain daripada computer sendiri. |
| (76) | *Public-Key Infrastructure*<br>(PKI) | Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perrkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet. |

| | | |
|---|---|---|
| (77) | Rahsia | Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing. |
| (78) | Rahsia Besar | Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia. |
| (79) | *Rollback* (undur) | Pengembalian pangkalan data atau program kepada keadaan stabil sebelum sesuatu ralat berlaku. |
| (80) | *Router* | Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet. |
| (81) | Ruang siber | Sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem tersebut secara fizikal atau maya serta persekitaran fizikal sistem-sistem tersebut dan semua aset yang berkaitan dengan ICT. |
| (82) | Sandaran *(Backup)* | Proses penduaan sesuatu dokumen atau maklumat. |
| (83) | *Screen saver* | Imej yang akan diaktifkan pada sistem/komputer setelah ianya tidak digunakan dalam jangka masa tertentu. |
| (84) | *Server* | Pelayan komputer |
| (85) | *Source Code* | Kod Sumber atau kod program (biasanya hanya dipanggil sumber atau kod) merujuk kepada sebarang siri pernyataan yang ditulis dalam bahasa pengaturcaraan komputer yang difahami manusia. |

| | | |
|---|---|---|
| (86) | Staf | Semua kategori pegawai yang sedang berkhidmat di UMPSA yang dilantik oleh Pihak Berkuasa Melantik SA secara tetap, sementara, kontrak *(Contract of Service)* dan *Contract for Service.* |
| (87) | Sulit | Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing. |
| (88) | Telekerja | Pekerjaan yang dijalankan di luar pejabat utama dengan menggunakan teknologi maklumat dan komunikasi. |
| (89) | *Threat* | Gangguan dan ancaman melalui pelbagai cara seperti e-mel dan surat yang bermotif peribadi dan atas sebab tertentu. |
| (90) | UMPSA CSIRT | *Computer Security Incident Response Team atau* Pasukan Tindak Balas Insiden Keselamatan ICT UMPSA. |
| (91) | *Uninterruptible Power Supply* (UPS) | Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung. |
| (92) | *Video Conference* | Media yang menerima dan memaparkan maklumat multimedia kepada pengguna pada masa yang sama ia diterima oleh penghantar. |
| (93) | *Video Streaming* | Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak. |

| | | |
|---|---|---|
| (94) | Virus | Atur cara yang bertujuan merosakkan data atau sistem aplikasi. |
| (95) | WAN | *Wide Area Network*<br>Rangkaian komputer jarak jauh dan teknologi yang biasanya digunakan untuk menyambungkan komputer yang berada pada lokasi yang berbeza (negeri, negara dan benua). WAN dalam skop UMPSA adalah sambungan kepada rangkaian internet. |
| (96) | Warga UMPSA | Staf dan pelajar UMPSA yang menggunakan perkhidmatan ICT UMPSA. |
| (97) | *Wireless LAN* | Jaringan komputer yang terhubung tanpa melalui kabel. |
| (98) | *Worm* | Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri, yang biasanya menjangkiti system operasi yang lemah atau tidak dikemas kini. |

## TUJUAN

Polisi Keselamatan Siber (PKS) Universiti Malaysia Pahang Al-Sultan Abdullah (UMPSA) ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA dalam melindungi maklumat di ruang siber.

## LATAR BELAKANG

Polisi ini dibangunkan untuk menjamin kesinambungan urusan UMPSA dengan meminimumkan kesan insiden keselamatan siber. Polisi ini akan memudahkan perkongsian maklumat sesuai dengan keperluan operasi UMPSA bagi memastikan semua maklumat dilindungi.

## OBJEKTIF

Objektif utama Polisi Keselamatan Siber ini dibangunkan adalah seperti yang berikut:

a. Menerangkan kepada semua pengguna merangkumi warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber;

b. Memastikan keselamatan penyampaian perkhidmatan UMPSA di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;

c. Memastikan kelancaran operasi UMPSA dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;

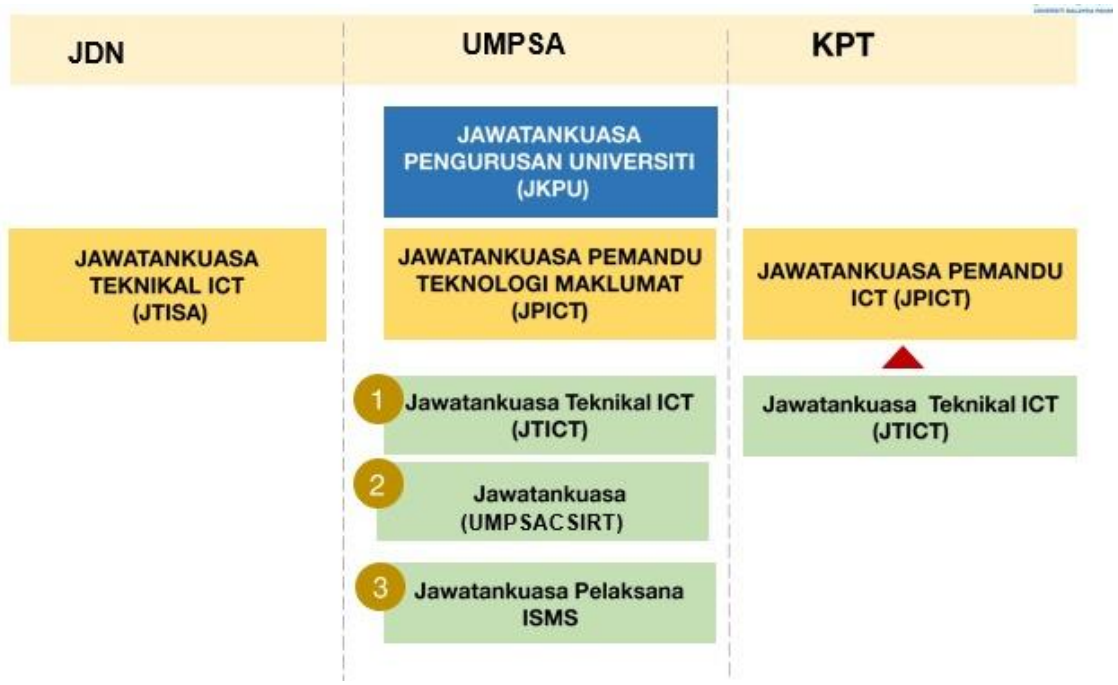
d. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan yang berlaku dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

e. Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

## TADBIR URUS

Bagi memastikan keberkesanan dan kejayaan pelaksanaan PKS UMPSA, satu (1) struktur tadbir urus iaitu Jawatankuasa Pemandu ICT (JPICT) UMPSA telah diwujudkan seperti berikut:

**CARTA JAWATANKUASA PELAKSANA ISMS UMPSA**




Rajah 1 : Struktur Jawatankuasa Pemandu ICT (JPICT)

**ASET ICT UMPSA**

1. Aset ICT UMPSA merangkumi Maklumat, Aliran Data, Platform Aplikasi dan Perisian, Peranti Fizikal dan Sistem, Sistem Luaran serta Sumber Luaran. Polisi ini meliputi semua sumber atau aset ICT yang digunakan seperti :

1.1. Maklumat

1.1.1. Semua penyedia perkhidmatan dalam UMPSA hendaklah mengenal pasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori :

a) Maklumat Rahsia Rasmi
Di bawah Akta Rahsia Rasmi 1972 (Akta 88), maksud Maklumat Rahsia Rasmi ialah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 (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 yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972.

b) Maklumat Rasmi
Maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh UMPSA semasa menjalankan urusan rasmi. Maklumat rasmi ini juga merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

c) Maklumat Pengenalan Peribadi
Maklumat Pengenalan Peribadi (PII atau Personally Identifiable Information) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu. PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

d) Data Terbuka

Data terbuka merujuk kepada data kerajaan yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan. PII dikecualikan daripada data terbuka.

1.2. Aliran Data

1.2.1. Aliran data merujuk kepada laluan lengkap data tertentu semasa transaksi. Aliran data dan komunikasi dalam UMPSA hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Saluran komunikasi termasuk :

a) Saluran komunikasi dan aliran data antara sistem di UMPSA;
b) Saluran komunikasi dan aliran data ke sistem luar; dan
c) Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

1.3. Platform Aplikasi dan Perisian

1.3.1. Semua platform aplikasi dan perisian hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

1.4. Peranti Fizikal dan Sistem

1.4.1. Semua peranti fizikal dan sistem hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Peranti fizikal termasuk:

a) Pelayan;
b) Peranti/Peralatan Rangkaian;
c) Komputer Peribadi/Komputer Riba;
d) Telefon/peranti pintar;
e) Media Storan;
f) Peranti dengan sambungan ke rangkaian, contohnya pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV);
g) Perkakasan teknologi untuk kegunaan pembelajaran,

pengajaran, pentadbiran dan penyelidikan;

h) Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi UMPSA; dan
i) Peranti pengesahan (*authentication devices*), contohnya token keselamatan, *dongle* dan alat pengimbas biometrik.

1.5. Sistem Luaran

1.5.1. Sistem luaran ialah sistem bukan milik UMPSA yang dihubungkan dengan sistem UMPSA. Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dinilai tahap keselamatannya secara berkala.

1.6. Sumber Luaran

1.6.1. Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkod dan dinilai tahap keselamatannya secara berkala. Perkhidmatan sumber luaran ialah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi UMPSA. Contoh perkhidmatan sumber luaran ialah:

a) Perisian Sebagai Satu Perkhidmatan
b) Platform Sebagai Satu Perkhidmatan
c) Infrastruktur Sebagai Satu Perkhidmatan
d) Storan Pengkomputeran Awan
e) Pemantauan Keselamatan

1.6.2. Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan, dikaji semula dan dipastikan keselamatannya secara berkala.

2. Semua perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

**RISIKO**

UMPSA hendaklah mengenal pasti risiko yang berkaitan dengan maklumat yang terlibat. Risiko ialah kebarangkalian UMPSA tidak dapat melaksanakan fungsi jabatan dengan baik. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam ruang siber UMPSA.

Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber UMPSA.

Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut :

a. Kerentanan *(Vulnerability)*

   Kerentanan adalah kelemahan atau kecacatan aset yang mungkin dieksploitasi dan mengakibatkan pelanggaran keselamatan. Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.

b. Ancaman

   UMPSA hendaklah mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

c. Impak

   UMPSA hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi UMPSA.

d. Tahap Risiko

   Tahap risiko ditentukan daripada ancaman, kebarangkalian dan impak risiko. Kaedah penentuan hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuat kuasa.

e. Penguraian Risiko *(Risk Treatment)*

   Penguraian risiko hendaklah dikenal pasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnya.

Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:

1. Teknologi
   Teknologi hendaklah dikenal pasti untuk mengurangkan risiko. Sebagai contoh, *firewall* digunakan untuk mengehadkan capaian logikal kepada sistem tertentu.

2. Proses
   Perekayasaan proses *(process reengineering)*, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

3. Manusia
   Mengenal pasti sumber manusia berkelayakan dan kompeten yang mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pengolahan risiko yang berkesan.

f. Pengurusan Risiko

   1. Penyedia perkhidmatan digital di UMPSA hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:
      i. mengenal pasti kerentanan;
      ii. mengenal pasti ancaman;
      iii. menilai risiko;
      iv. menentukan penguraian risiko;
      v. memantau keberkesanan penguraian risiko; dan
      vi. memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

Tahap risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya sekali setahun dan dimaklumkan kepada Mesyuarat Jawatankuasa Pelaksana ISMS UMPSA.

## PRINSIP KESELAMATAN

Prinsip – prinsip yang menjadi asas Polisi Keselamatan Siber UMPSA dan perlu dipatuhi adalah seperti berikut:

a) Prinsip “Perlu-Tahu”

UMPSA hendaklah melaksanakan mekanisme bagi memberikan kebenaran kepada capaian maklumat. Maklumat yang dicapai oleh pengguna yang dibenarkan hendaklah berdasarkan prinsip “Perlu-Tahu” yang membenarkan capaian maklumat yang diperlukan untuk melaksanakan tugasnya sahaja.

Bagi capaian spesifik Maklumat Rahsia Rasmi, penggunaan yang dibenarkan hendaklah dihadkan kepada masa, lokasi, peranan dan fungsi pengguna tersebut.

b) Hak Keistimewaan minimum

Pengguna hendaklah diberikan hak keistimewaan minimum iaitu terhad 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 mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Prinsip ini digunakan untuk menyekat hak akses kepada aplikasi, sistem, proses dan peranti kepada pengguna yang dibenarkan untuk melaksanakan aktiviti. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

c) Pengasingan Tugas

Bagi mengekalkan prinsip semak-dan-imbang *(check and balance)*, UMPSA hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

d) Kawalan Capaian Berdasarkan Peranan

Capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut.

e) Peminimuman Data

UMPSA hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut.

## TEKNOLOGI

Teknologi untuk melindungi data hendaklah dikenal pasti di semua peringkat pemprosesan data di setiap elemen pengkomputeran seperti berikut :

1.1 Peringkat Pemprosesan Data

1.1.1 Data-dalam-simpanan

a) UMPSA hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-simpanan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-simpanan.

b) Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII perlu dilindungi daripada segi kerahsiaan dan integriti data. Data terbuka perlu dilindungi daripada segi integriti data.

1.1.2 Data-dalam-pergerakan

UMPSA hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-pergerakan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data dalam-pergerakan.

1.1.3 Data-dalam-penggunaan

a) UMPSA hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-penggunaan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Di samping itu, teknologi untuk menentukan asal data dan tanpa sangkalan mungkin diperlukan. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data dalam penggunaan.

b) Teknologi yang bersesuaian boleh digunakan oleh UMPSA untuk memastikan asal data dan data/transaksi tanpa-sangkal.

1.1.4 Perlindungan Ketirisan Data

a) Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.

b) Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

1.2 Elemen dalam Persekitaran Pengkomputeran

Berdasarkan penilaian risiko dan pelan pengurusan risiko, UMPSA hendaklah menggunakan kaedah teknologi dan kawalan keselamatan *(counter measure dan control measure)* yang dapat melindungi data di semua peringkat saluran pemprosesan bagi semua elemen dalam persekitaran pengkomputeran.

Maklumat Rahsia Rasmi hendaklah disimpan dan diproses dalam persekitaran pengkomputeran mengikut Arahan Keselamatan yang dikeluarkan oleh Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) atau mendapat pengesahan dari CGSO.

Maklumat UMPSA hendaklah disimpan dan diproses dalam persekitaran penghomputeran mengikut prosedur yang sedang berkuatkuasa di UMPSA.

**PROSES**

Warga UMPSA hendaklah melindungi keselamatan siber dengan melaksanakan perkara-perkara berikut:

1.1 Konfigurasi Asas

1.1.1 Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem.

1.1.2 Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.

1.2 Kawalan Perubahan Konfigurasi

1.2.1 Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.

1.2.2 Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini.

1.2.3 Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.

1.3 Sandaran *(backup)*

1.3.1 Sandaran (backup) hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan.

1.3.2 Media sandaran *(backup)* hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.

1.4 Kitaran Pengurusan Aset

1.4.1 Pindah

1.4.1.1 Pemindahan hak milik aset berlaku dalam keadaan berikut :

a) Warga UMPSA meninggalkan agensi disebabkan oleh persaraan, perletakan jawatan atau penugasan semula;
b) Aset yang dikongsi untuk kegunaan sementara;
c) Pemberian aset kepada agensi lain; dan
d) Aset dikembalikan setelah tamat tempoh sewaan.

1.4.1.2 Data dalam peranti tersebut hendaklah diuruskan mengikut tatacara pelupusan di perkara (1.4.2).

1.4.2 Pelupusan

1.4.2.1 Pelupusan media storan perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh UMPSA;

1.4.2.2 Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.

1.4.2.3 Pelupusan juga perlu dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara 2003 [Akta 629] dan Peraturan-Peraturan Arkib Negara (Penetapan Borang-Borang bagi Pelupusan Rekod Awam) 2008 [P.U. (A) 377/2008].

1.4.2.4 Pelupusan boleh dalam bentuk pemusnahan fizikal dan/atau sanitasi data.

1.4.2.5 Sanitasi data hendaklah mengikut Garis Panduan Sanitasi Media Elektronik Sektor Awam yang sedang berkuat kuasa.

1.4.3 Kitaran Hayat

1.4.3.1 Kitaran hayat data adalah tertakluk kepada peruntukan di bawah Akta 629.

1.4.3.2 Pelupusan rekod urusan am universiti hendaklah diuruskan mengikut Jadual Pelupusan Rekod Urusan Am.

1.4.3.3 Pelupusan rekod kewangan dan perakauan universiti hendaklah diuruskan mengikut Jadual Pelupusan Rekod Kewangan dan Perakaunan 2023.

**MANUSIA**

Warga UMPSA, pembekal, pakar runding dan pihak-pihak yang berkepentingan hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta undang-undang dan peraturan semasa yang berkuatkuasa.

Sistem penyampaian perkhidmatan UMPSA hendaklah dikendalikan oleh individu yang kompeten dan berpengetahuan. Staf UMPSA hendaklah dilatih dalam bidang pengkhususan yang diperlukan. Asas kecekapan pengguna hendaklah dibangunkan bagi semua warga UMPSA.

1.1 Kompetensi Pengguna

1.1.1 Kompetensi pengguna termasuk :

a) Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan siber dengan mewujudkan komunikasi ICT dan program kesedaran keselamatan siber.
b) Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada warga UMPSA berhubung alat-alat keselamatan berkaitan untuk memastikan mereka mampu untuk melaksanakan tugas harian mereka.
c) Kompetensi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian mendalam.
d) Setiap orang yang diberi kuasa untuk mengendalikan dokumen terperingkat, kompetensi tambahan pengguna selaras dengan arahan/ pekeliling semasa adalah diharapkan.

1.2 Kompetensi Pelaksana

1.2.1 Warga UMPSA yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

1.2.2 Pegawai Keselamatan ICT hendaklah memenuhi syarat-syarat berikut :

a) Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber.
b) Memenuhi keperluan pembelajaran berterusan.

c) Menimba pengalaman yang mencukupi dalam bidang keselamatan siber.
d) Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa.

1.3 Peranan

1.3.1 Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.

1.3.2 Semua pihak yang berurusan dengan Maklumat Terperingkat hendaklah menjaga kerahsiaan maklumat tersebut dan menandatangani akujanji/ perjanjian kerahsiaan mengikut prosedur yang berkenaan. Salinan asal akujanji/perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan.

1.3.3 Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.

1.3.4 Staf UMPSA yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT di PTJ dikembalikan sekiranya berlaku perubahan peranan.

1.3.5 Staf UMPSA yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset ICT di PTJ yang berkaitan seperti tersenarai dalam senarai aset dalam Nota Serah Tugas.

1.3.6 Staf UMPSA lain yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset ICT di PTJ dengan diselia oleh staf yang dipertanggungjawabkan.

## PELAN PENGURUSAN KESELAMATAN MAKLUMAT

1. Setiap projek di UMPSA hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain.
2. Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), Polisi Keselamatan Siber UMPSA dan surat pekeliling/arahan terkini untuk menangani isu-isu operasi projek.
3. Pelan ini hendaklah mengenal pasti perlindungan data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data.
4. Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah :

    4.1 Peranti pengkomputeran peribadi

        4.1.1 Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja, telefon pintar, tablet, dan peranti storan.

        4.1.2 Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Terperingkat hendaklah memohon kebenaran daripada pihak bertanggungjawab di UMPSA. Walau bagaimanapun, peranti pengkomputeran peribadi milik pensendirian hendaklah dilarang daripada mencapai Maklumat Terperingkat.

    4.2 Peranti rangkaian

        4.2.1 Merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti suis, penghala, *firewall*, peranti VPN dan kabel.

        4.2.2 Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

4.3 Aplikasi

4.3.1 Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi, sistem operasi.

4.3.2 Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

4.4 Pelayan

4.4.1 Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.

4.4.2 Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

4.5 Persekitaran fizikal

4.5.1 Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

4.5.2 UMPSA hendaklah merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

4.5.3 Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip *defence-in-depth*.

4.5.4 Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

## PERNYATAAN POLISI KESELAMATAN SIBER UMPSA

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan dan melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan siber sentiasa berubah.

Pernyataan ini merangkumi perlindungan semua bentuk maklumat elektronik dan bukan elektronik yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bagi memelihara keselamatan ruang siber dan ketersediaan maklumat kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut :

1. **Kerahsiaan**
   Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.

2. **Integriti**
   Data dan maklumat hendaklah tepat, lengkap dan kemas kini dan hanya boleh diubah dengan cara yang dibenarkan.

3. **Tidak Boleh Disangkal**
   Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal.

4. **Kesahihan**
   Data dan maklumat hendaklah dipastikan kesahihannya.

5. **Ketersediaan**
   Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain itu, langkah-langkah ke arah memelihara keselamatan siber hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan ICT UMPSA, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah- langkah pencegahan yang perlu diambil untuk menangani risiko berkenaan.

EMPAT (4) kawalan yang terlibat di dalam Polisi Keselamatan Siber UMPSA diterangkan dengan lebih jelas dan teratur dalam dokumen ini seperti berikut :

| 5 KAWALAN ORGANISASI *(ORGANIZATIONAL CONTROLS)* | |
|---|---|
| **5.1 POLISI KESELAMATAN MAKLUMAT *(POLICIES FOR INFORMATION SECURITY)*** | |
| **PERKARA** | **TANGUNGJAWAB** |
| 5.1.1 **Jawatankuasa Pemandu ICT (JPICT)** adalah jawatankuasa yang bertanggungjawab ke atas pelaksanaan Polisi Keselamatan Siber UMPSA berasaskan lantikan daripada Naib Canselor UMPSA. | JPICT, CIO, ICTSO dan Pelaksana ICT |
| 5.1.2 Pelaksanaan polisi ini akan dijalankan oleh UMPSA dengan disokong oleh Jawatankuasa Pelaksana ISMS yang terdiri daripada:<br>a) Pengerusi ISMS (CIO)<br>b) Pegawai Keselamatan ICT (ICTSO)<br>c) Ahli-ahli yang dilantik oleh UMPSA<br><br>Polisi ini perlu disebarkan dan dipatuhi oleh semua warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA.<br><br>Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh UMPSA kepada warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA. | JPICT, CIO, ICTSO dan Pelaksana ICT |
| 5.1.3 Polisi Keselamatan Siber ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, polisi kerajaan dan kepentingan organisasi serta sosial. Berikut adalah prosedur yang berkaitan dengan kajian semula Polisi Keselamatan Siber UMPSA : | JPICT, CIO, ICTSO dan Pelaksana ICT |

| | |
|---|---|
| a) Mengenal pasti dan menentukan perubahan yang diperlukan;<br>b) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO atau Jawatankuasa Teknikal ICT (JTICT) untuk tindakan dan pertimbangan kepada JPICT bagi tujuan pengesahan;<br>c) Memaklumkan kepada semua warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA berkenaan pindaan yang telah diluluskan dan disahkan oleh JPICT; dan<br>d) Polisi ini hendaklah dikaji semula **sekurang-kurangnya LIMA (5) tahun sekali** atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan. | |

## 5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*

### 5.2.1 NAIB CANSELOR UMPSA

Peranan dan tanggungjawab Naib Canselor UMPSA adalah seperti berikut:

a) Memastikan penguatkuasaan pelaksanaan Polisi ini;
b) Mempertimbangkan/meluluskan semua keperluan ICT UMPSA seperti sumber kewangan, sumber manusia dan perlindungan keselamatan adalah mencukupi melalui cadangan atau perancangan yang disediakan oleh Ketua Pegawai Maklumat (CIO); dan
c) Melantik CIO dan ICTSO.

**5.2.2 KETUA PEGAWAI MAKLUMAT (CIO)**

Peranan dan tanggungjawab CIO adalah seperti yang berikut:

a) Membantu Naib Canselor dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan di dalam Polisi ini;
b) Merancang dan memastikan semua keperluan ICT UMPSA seperti sumber kewangan, sumber manusia dan perlindungan keselamatan adalah mencukupi;
c) Memastikan kawalan keselamatan maklumat dalam UMPSA diseragam dan diselaraskan dengan sebaiknya;
d) Memastikan Pelan Strategik ICT UMPSA mengandungi aspek keselamatan siber; dan
e) Menyelaras pelan latihan dan program kesedaran keselamatan siber.

**5.2.3 PEGAWAI KESELAMATAN ICT (ICTSO)**

Peranan dan tanggungjawab ICTSO adalah seperti berikut:

a) Mempengerusikan Jawatankuasa Keselamatan Siber UMPSA;
b) Merancang dan merangka pematuhan dan pelaksanaan PKS UMPSA;
c) Merancang dan merangka Sistem Pengurusan Keselamatan Maklumat termasuk Pengurusan Risiko dan Audit Keselamatan Maklumat;
d) Merancang dan merangka pengurusan insiden Keselamatan Siber;
e) Merancang dan merangka penilaian tahap Keselamatan Siber;
f) Melaporkan insiden Keselamatan Siber kepada pihak National Cyber Security Agency (NACSA) dan seterusnya membantu dalam penyiasatan atau pemulihan;
g) Melaporkan insiden Keselamatan Siber kepada CIO/CDO bagi insiden yang memerlukan Pengurusan Kesinambungan Perkhidmatan (PKP);
h) Menyemak, memantau, mengkaji dan menyediakan analisa laporan berkaitan dengan isu-isu Keselamatan Siber UMPSA; dan
i) Merancang dan merangka program kesedaran Keselamatan Siber dan merangka penyebaran amaran-amaran yang sesuai terhadap kemungkinan berlaku ancaman kepada Keselamatan Siber UMPSA.

**5.2.4 KETUA PUSAT TANGGUNGJAWAB**

Peranan dan tanggungjawab Ketua Pusat Tanggungjawab adalah seperti berikut:

a) Menentukan kawalan keselamatan ICT selaras dengan keperluan UMPSA;
b) Merancang semua warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA mematuhi dasar, piawaian, prosedur dan garis panduan keselamatan ICT UMPSA;
c) Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat yang berkuat kuasa;
d) Melaksanakan pematuhan Polisi ini oleh warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA;
e) Memastikan warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini;
f) Menentukan kawalan akses semua pengguna terhadap aset ICT UMPSA.

### 5.2.5 PENGURUS ICT

Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

a) Memastikan Polisi Keselamatan Siber UMPSA dilaksanakan dan dipatuhi di bahagian dan jabatan;

b) Memastikan semua pengguna UMPSA mematuhi dasar, piawaian dan garis panduan keselamatan ICT, dan seterusnya melaporkan sebarang insiden berkaitan keselamatan ICT;

c) Mengkaji semula aspek-aspek keselamatan fizikal seperti kemudahan *backup* dan persekitaran pejabat yang perlu,

d) Melaksanakan keperluan Polisi Keselamatan Siber dalam operasi semasa seperti berikut:

   i. Pelaksanaan sistem atau aplikasi baru sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru;
   ii. Pembelian atau peningkatan perisian dan sistem komputer;
   iii. Perolehan teknologi dan perkhidmatan komunikasi baru;
   iv. Pelantikan pembekal, perunding atau rakan usahasama; dan
   v. Menentukan pembekal, perunding atau rakan usahasama menjalani tapisan keselamatan selaras dengan keperluan tahap perkhidmatan.

e) Memastikan bentuk ancaman keselamatan terkini dikenalpasti dan penemuan ancaman dilaporkan kepada ICTSO;

f) Menyemak dan mengesahkan garis panduan, prosedur dan tatacara bagi semua aplikasi yang dibangunkan di bahagian-bahagian agar mematuhi keperluan Polisi Keselamatan Siber UMPSA;

g) Membangun, mengkaji semula dan mengemas kini pelan kontingensi dengan mengaktifkan Pelan Pemulihan Bencana (DRP); dan

h) Memastikan sistem kawalan capaian pengguna ke atas aset-aset ICT UMPSA dilaksanakan.

**5.2.6 PENTADIR ICT / PEMILIK ASET ICT**

Pentadbir ICT ialah semua Ketua Bahagian ICT / Ketua Seksyen ICT / Ketua Unit ICT / Pegawai Penyelia/ Ketua Teknikal ICT di UMPSA dan Pemilik Aset ICT pula adalah wakil-wakil PTJ yang memiliki dan menguruskan aset ICT UMPSA yang berperanan dan bertanggungjawab dalam melaksanakan keperluan Polisi ini dalam operasi ICT UMPSA semasa seperti yang berikut:

a) Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu;
b) Pembelian atau peningkatan perisian dan sistem komputer;
c) Perolehan teknologi dan perkhidmatan komunikasi baru;
d) Menentukan pembekal dan rakan usaha sama mematuhi Polisi ini;
e) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini;
f) Memastikan semua aset ICT dikenalpasti dan diklasifikasikan berdasarkan nilai dan keperluan keselamatan;
g) Melakukan penilaian risiko secara berkala terhadap aset yang dimiliki dan mengambil tindakan mitigasi yang sesuai;
h) Mengimplementasikan langkah-langkah keselamatan yang diperlukan untuk melindungi aset daripada ancaman dan serangan;
i) Menyedia dan melaksana latihan dan program kesedaran keselamatan siber; dan
j) Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat kerajaan yang berkuatkuasa.

**5.2.7 PELAKSANA ICT (SISTEM APLIKASI)**

Peranan dan tanggungjawab Pelaksana Sistem Aplikasi/Perkhidmatan Digital adalah seperti berikut:

a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai staf yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;
b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi ini;
c) Memantau aktiviti capaian sistem aplikasi;
d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;
e) Menganalisis dan menyimpan rekod jejak audit;
f) Menyediakan laporan mengenai aktiviti capaian secara berkala;
g) Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas;
h) Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaanya;
i) Memastikan *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemaskini supaya terhindar daripada ancaman virus dan penggodam;
j) Mematuhi dan melaksanakan prinsip-prinsip Polisi ini dalam pengujudan akaun pengguna ke atas setiap sistem aplikasi;
k) Memastikan *backup* sistem aplikasi dan data yang berkaitan dengannya dibuat secara berjadual;
l) Menghadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan dari penyalahgunaannya;
m) Melaporkan kepada UMPSA CSIRT jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya;

**5.2.8 PELAKSANA ICT (TEKNIKAL)**

Peranan dan tanggungjawab Pelaksana Teknikal adalah seperti berikut :

a) Menyediakan khidmat sokongan teknikal ICT;
b) Merancang dan melaksanakan perolehan aset ICT;
c) Mengurus pendaftaran, agihan, penempatan dan pelupusan Aset ICT;
d) Memastikan semua aset ICT diselenggarakan secara berkala dengan sempurna;
e) Memastikan perisian antivirus dipasang pada Aset ICT; dan
f) Mengurus Meja Bantuan ICT UMPSA;

**5.2.9 PELAKSANA ICT (RANGKAIAN)**

Peranan dan tanggungjawab Pelaksana Rangkaian adalah seperti berikut :

a) Memastikan rangkaian setempat (LAN), rangkaian luas (WAN) dan rangkaian Wireless UMPSA beroperasi sepanjang masa;
b) Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna;
c) Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada;
d) Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil dan sebarang kerosakan perkakasan sokongan rangkaian UMPSA;
e) Memantau penggunaan rangkaian dan melaporkan kepada UMPSA CSIRT sekiranya berlaku penyalahgunaan sumber rangkaian;
f) Mewartakan polisi dan garis panduan penggunaan rangkaian UMPSA kepada pengguna rangkaian;
g) Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan luar ke dalam rangkaian UMPSA secara tidak sah; dan
h) Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian.

**5.2.10 PELAKSANA ICT (LAMAN WEB / PORTAL *(WEBMASTER)*)**

Peranan dan tanggungjawab pelaksana Laman Web adalah seperti berikut:

a) Menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah;

b) Memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar;

c) Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman;

d) Menghadkan capaian Pentadbir Laman Web bahagian/unit ke web server;

e) Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi;

f) Melaporkan sebarang pelanggaran keselamatan laman portal kepada UMPSA CSIRT.

**5.2.11 PELAKSANA ICT (E-MEL)**

Peranan dan tanggungjawab pelaksana E-Mel adalah seperti berikut:

a) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Ketua Jabatan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar Polisi dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat;

b) Pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib;

c) Menyimpan jejak audit selama sekurang-kurangnya enam (1) bulan di dalam pelayan e-mel ATAU tertakluk kepada kemampuan ruang storan;

d) Melaksanakan jadual penstoran dan pengarkiban e-mel. Penyimpanan media storan sama ada di luar atau di dalam kawasan mestilah mempunyai ciri-ciri keselamatan fizikal yang terjamin bagi mengelak daripada sebarang risiko seperti kehilangan maklumat;

e) Memastikan akaun e-mel pengguna sentiasa dalam keadaan baik dan berfungsi;

f) Memastikan keselamatan akaun e-mel pengguna dari ancaman luar dan dalam;

g) Melaksanakan penyelenggaraan ke atas sistem e-mel dengan baik dan menentukan segala *patches* terkini yang disediakan oleh pihak pembekal dipasang dan berfungsi dengan sempurna;

h) Memantau status storan e-mel Pengurusan Atasan UMPSA dan memastikan emel Pengurusan Atasan UMPSA sentiasa tersedia untuk transaksi e-mel;

i) Memastikan semua peralatan sistem e-mel sentiasa aktif 24 x 7;

j) Memastikan agar keupayaan *mail relay* hanya boleh digunakan untuk server atau aplikasi dalaman UMPSA sahaja bagi tujuan keselamatan;

k) Memastikan kemudahan membuat capaian e-mel melalui pelbagai media seperti telefon mudah alih disediakan kepada pengguna e-mel UMPSA; dan

l) Memastikan pengguna e-mel UMPSA berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel UMPSA dan Internet serta pelaksanaan aktiviti Pembudayaan ICT

(Penggunaan E-mel dan Internet) secara berterusan melalui latihan serta promosi.

**5.2.12 PELAKSANA ICT (PUSAT DATA DAN *DISASTER RECOVERY CENTER (DRC)*)**

Peranan dan tanggungjawab pegawai adalah seperti berikut :

a) Memastikan Operasi Pusat Data dan DRC berada dalam keadaan baik 24 x 7;

b) Merancang dan menyelia pelaksanaan simulasi *Disaster Recovery Plan (DRP)* UMPSA;

c) Pengurus operasi DRC sekiranya berlaku bencana terhadap Pusat Data UMPSA;

d) Memastikan Operasi Infrastruktur Virtualisasi di Pusat Data dan DRC berfungsi dan diselenggara dengan baik bagi meningkatkan jangka hayat perkhidmatan perkakasan serta perisian;

e) Memastikan Operasi *Backup / Restore* Data berfungsi dan diselenggara dengan baik bagi meningkatkan jangka hayat perkhidmatan perkakasan serta perisian;

f) Memantau Aset ICT sokongan dan Fasiliti Sokongan (*Precision Aircond,* Alat Pencegah Kebakaran, Alarm, Bekalan Elektrik) di Pusat Data dan DRC bagi memastikan beroperasi lancar 24 x 7;

g) Menguruskan permohonan baru dan pengemaskinian server dan *Virtual Machine* bagi sistem aplikasi baru di Pusat Data dan DRC;

h) Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian- perisian lain di web server; dan pusat data dan

i) Menguruskan Khidmat Sokongan Operasi Server dari segi Penerimaan, Penyediaan, Penyelenggaraan, Waranti, Pengeluaran dan Pelupusan

**5.2.13 PEGAWAI ASET ICT**

Peranan dan tanggungjawab pegawai aset ICT adalah seperti berikut :

a) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik;
b) Memastikan Aset ICT milik UMPSA dilabel dan direkodkan ke dalam Sistem Pengurusan Aset;
c) Memastikan Aset milik UMPSA dibuat pemeriksaan berkala secara tahunan dan diselenggara sebaiknya agar dapat meningkatkan jangka hayat Aset ICT tersebut;
d) Memastikan Aset ICT untuk pinjaman dan simpanan sebelum agihan diletakkan di dalam bilik stor yang mempunyai kawalan keselamatan yang terjamin;
e) Memastikan Stok alat ganti Aset ICT sentiasa mencukupi dan disimpan di tempat yang selamat dan terkawal; dan
f) Memastikan Aset ICT yang ingin dilupuskan dilaksanakan mengikut garis panduan kawalan keselamatan bagi pelupusan data digital.

**5.2.14 JAWATANKUASA PEMANDU ICT (JPICT)**

Peranan dan tanggungjawab JPICT adalah seperti yang berikut:

a) JPICT berperanan bagi menetapkan hala tuju, strategi perlaksanaan ICT dan sumber-sumber di UMPSA;
b) JPICT memantau urusan perkembangan dan pemantauan aktiviti ICT di UMPSA;
c) JPICT juga turut berperanan untuk menyelaras permohonan projek ICT di UMPSA;
d) JPICT bertanggungjawab sepenuhnya dalam melaporkan hal ehwal pengurusan dan penyelarasan berkaitan ICT kepada Jawatankuasa Pengurusan Universiti (JKPU) UMPSA;
e) JPICT UMPSA juga turut sebagai penghubung dan melaporkan kepada JPICT dan JTICT bagi Kementerian Pendidikan Malaysia dan JTICT MAMPU bagi permohonan dan perolehan berkaitan ICT;
f) JPICT juga adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT UMPSA;
g) Bidang kuasa JPICT di dalam keselamatan ICT UMPSA termasuk memantau tahap pematuhan keselamatan ICT, memperakukan polisi, dasar, prosedur, garis panduan dan tatacara, dan memastikan pemakaian pekeliling-pekeliling serta arahan kerajaan semasa; dan
h) Berikut adalah Terma dan Rujukan JPICT:
    i. Merangka, menggubal dan meluluskan peraturan dan dasar ICT UMPSA;
    ii. Merangka, merancang dan menetapkan hala tuju dan strategi untuk perlaksanaan ICT UMPSA;
    iii. Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan hala tuju dan strategi ICT UMPSA;
    iv. Merangka dan merancang perlaksanaan program dan projek ICT UMPSA supaya selaras dengan Pelan Strategik ICT UMPSA;
    v. Merancang dan menetapkan langkah-langkah keselamatan ICT dan Polisi Keselamatan Siber di UMPSA;
    vi. Menilai dan meluluskan projek ICT berdasarkan kepada

keperluan sebenar dan dengan perbelanjaan berhemah serta mematuhi peraturan semasa; dan

vii. Melapor perkembangan projek, aktiviti, program dan pelaksanaan ICT kepada Jawatankuasa Pengurusan Universiti (JKPU) mengikut keperluan.

**5.2.15 JAWATANKUASA TEKNIKAL ICT (JTICT)**

Peranan dan tanggungjawab JTICT adalah seperti yang berikut:

a) Jawatankuasa Teknikal Teknologi Maklumat (JTICT) merupakan sebuah jawatankuasa yang ditubuhkan di bawah JPICT bagi menimbang, membincang dan meluluskan permohonan kelulusan dari aspek teknikal/spesifikasi ICT yang melibatkan perolehan sistem, rangkaian, perkakasan dan perisian ICT yang dipohon atau dicadangkan oleh PTJ berkaitan.

b) Berikut adalah Terma dan Rujukan JTICT:

i. Menyelaras hala tuju dan strategi ICT UMPSA;

ii. Mengenal pasti, menilai dan menimbang sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju dan strategi ICT UMPSA;

iii. Menyelaras pelaksanaan program dan projek-projek ICT supaya selaras dengan Pelan Strategik UMPSA;

iv. Menilai dan memperakukan semua perolehan ICT di UMPSA;

v. Menyelaras langkah-langkah keselamatan ICT di UMPSA;

vi. Menimbang, meneliti, menilai dan memberi kelulusan proses perolehan cadangan spesifikasi teknikal dalam Jadual Penentuan Teknikal skop ICT; dan

vii. Mengikuti dan memantau perkembangan program ICT di UMPSA serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT.

**5.2.16 JAWATANKUASA PELAKSANA ISMS**

Peranan dan tanggungjawab Jawatankuasa Pelaksana ISMS adalah seperti berikut:

a) Menentukan hala tuju keseluruhan pelaksanaan pensijilan ISMS UMPSA yang merangkumi perancangan, pemantauan dan pegesahan terhadap perkara-perkara berikut:
   i. Pelaksanaan pensijilan ISMS ke atas perkhidmatan UMPSA yang dikenalpasti;
   ii. Kelulusan ke atas dasar, objektif, dan skop pelaksanaan ISMS;
   iii. Penetapan kriteria penerimaan risiko, tahap risiko dan *risk treatment plan*
b) Keputusan dan tindakan Mesyuarat Jawatankuasa Pelaksana ISMS UMPSA dan mesyuarat-mesyuarat yang berkaitan ISMS;
c) Kajian semula pelaksanaan pensijilan ISMS ke atas perkhidmatan-perkhidmatan UMPSA yang dikenal pasti;
d) Dasar dan objektif ISMS diwujudkan selaras dengan hala tuju strategik UMPSA;
e) Keperluan ISMS diterapkan dalam budaya kerja staf UMPSA;
f) Sumber yang diperlukan oleh pasukan pelaksana ISMS;
g) Kepentingan pengurusan ISMS yang berkesan dan pematuhan terhadap keperluannya;
h) Pencapaian sasaran ISMS seperti yang dirancang;
i) Arahan dan sokongan kepada pasukan JK Pelaksana ISMS UMPSA bagi memastikan ISMS dapat dilaksanakan dengan berkesan;
j) Pelaksanaan program penambahbaikan dan peningkatan ISMS yang berterusan; dan
k) Meluluskan:
   i. Struktur Organisasi ISMS UMPSA;
   ii. Keperluan sumber; dan
   iii. Pelantikan Pasukan Audit Dalam ISMS UMPSA

**5.2.17 PASUKAN UMPSA CSIRT (*COMPUTER SECURITY INCIDENT RESPONSE TEAM)***

Peranan dan Tanggungjawab UMPSA CSIRT adalah seperti berikut :

a) Menerima dan mengesan aduan keselamatan siber dan menilai tahap dan jenis insiden;

b) Merekodkan dan menjalankan siasatan awal insiden yang diterima;

c) Menangani tindak balas (*response*) insiden keselamatan siber dan mengambil tindakan baik pulih minima;

d) Menasihati Pengurus/ Pentadbir/ Pelaksana/ Pemilik Aset ICT untuk mengambil tindakan pemulihan dan pengukuhan;

e) Menyebarkan makluman berkaitan pengukuhan keselamatan siber kepada Pengurus/ Pentadbir/ Pelaksana/ Pemilik Aset ICT; dan

f) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.

**5.2.18 PENGGUNA**

Peranan dan tanggungjawab pengguna adalah seperti berikut:

a) Membaca, memahami dan mematuhi Polisi ini;

b) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya;

c) Menjalani tapisan keselamatan sekiranya diperlukan dikehendaki berurusan dengan maklumat rasmi terperingkat;

d) Mematuhi prinsip-prinsip Polisi ini dan menjaga kerahsiaan maklumat UMPSA dan Kerajaan;

e) Melaksanakan langkah-langkah perlindungan seperti berikut :-

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;

iii. Menentukan maklumat sedia untuk digunakan;

iv. Menjaga kerahsiaan kata laluan;

v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan siber yang ditetapkan;

vi. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

vii. Menjaga kerahsiaan bagi setiap langkah-langkah keselamatan siber dari diketahui umum.

f) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada Pasukan UMPSA CSIRT dengan segera;

g) Menghadiri program-program kesedaran mengenai keselamatan siber ; dan

h) Bersetuju dengan terma dan syarat yang terkandung di dalam Polisi ini dengan menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber UMPSA sebagaimana **Lampiran 2.**

| **5.3 PENGASINGAN TUGAS *(SEGREGATION OF DUTIES)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang | Pengurus ICT, Pentadbir ICT dan Pelaksana ICT |

| | |
|---|---|
| mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset.<br>Perkara - perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;<br>b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi;<br>c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai production. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan<br>d) Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya. | |

| **5.4 TANGGUNGJAWAB PENGURUSAN *(MANAGEMENT RESPONSIBILITIES)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Ketua Jabatan atau pegawai berkaitan hendaklah memastikan staf UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA supaya mengamalkan | Ketua PTJ yang berkaitan, Warga UMPSA, pembekal, pakar runding dan pihak yang |

| | |
|---|---|
| keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.<br><br>Ketua Jabatan atau pegawai yang bertanggungjawab perlu memastikan setiap warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber UMPSA. | mempunyai urusan dengan perkhidmatan ICT UMPSA |

| **5.5 HUBUNGAN DENGAN PIHAK BERKUASA *(CONTACT WITH AUTHORITIES)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab UMPSA;<br>b) Mewujud dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia, Agensi Keselamatan Siber Negara (NACSA), Suruhanjaya Komunikasi Dan Multimedia atau pihak lain yang berkaitan. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan<br>c) Insiden keselamatan maklumat harus | Pasukan UMPSA CSIRT, PTJ berkaitan dan pihak yang telibat |

| | |
|---|---|
| dilaporkan tepat pada masanya bagi mengurangkan impak insiden. | |

| **5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS *(CONTACT WITH SPECIAL INTEREST GROUPS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau pun forum bagi:<br>a) Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat;<br>b) Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini; dan<br>c) Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat. | Warga UMPSA (Mengikut Bidang Kepakaran) |

| **5.7 ANCAMAN PERISIKAN *(THREAT INTELLIGENCE)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Teknologi Informasi dan Komunikasi (ICT) adalah serangkaian langkah dan tindakan yang diambil untuk mengesan, melindungi, dan mencegah berbagai jenis ancaman perisikan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Sistem pemantauan (*Security Monitoring*) bagi mengesan aktiviti yang | Pentadbir ICT dan Pelaksana ICT |

| | |
|---|---|
| mencurigakan atau ancaman perisikan yang mungkin terjadi di dalam rangkaian atau sistem;<br>b) Memasang *firewall* bagi mengawal lalu lintas jaringan rangkaian daripada aktiviti yang mencurigakan;<br>c) Data yang disimpan hendaklah dienkripsi (*Encryption*) bagi melindungi data daripada dicapai oleh orang tidak sah jika ada keperluan;<br>d) Mengawal akses setiap pengguna aplikasi rangkaian atau sistem mengikut skop tugas yang telah ditetapkan oleh PTJ;<br>e) Membahagikan rangkaian di dalam sesebuah organisasi kepada bebarapa bahagian mengikut tingkat atau sebagainya; dan<br>f) Mengkaji, menilai dan mengemaskini teknologi perkakasan atau perisian mengikut kesesuaian keadaan semasa. | |

| **5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK *(INFORMATION SECURITY IN PROJECT MANAGEMENT)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek di UMPSA;<br>b) Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;<br>c) Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan- | Warga UMPSA (Pasukan Projek), pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| | |
|---|---|
| kawalan yang diperlukan; dan<br>d) Kontrak hendaklah mengandungi terma-terma yang relevan bagi tujuan keselamatan maklumat seperti keperluan di dalam Polisi Keselamatan Siber UMPSA; dan<br>e) Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat atau perlu mematuhi keperluan di dalam pensijilan keselamatan maklumat.<br><br>2. 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:<br>a) Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk pengkonsepan perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penyelenggaraan dan pelupusan;<br>b) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Polisi Keselamatan Siber UMPSA;<br>c) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan | |

| | |
|---|---|
| d) Ujian keselamatan hendaklah dilakukan semasa pembangunan sIstem bagi memastikan kesahihan dan integriti data. | |

| **5.9 MAKLUMAT INVENTORI ASET DAN YANG BERKAITAN *(INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT UMPSA. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut:<br>a) UMPSA hendaklah mengenal pasti Pegawai Penerima Aset setiap PTJ untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT;<br>b) Pegawai Pemeriksa Aset hendaklah memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara dan dilupuskan. Maklumat aset direkodkan dan sentiasa dikemaskini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa;<br>c) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;<br>d) Pegawai Aset hendaklah mengesahkan penempatan aset ICT;<br>e) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan<br>f) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya. | Pegawai Aset, Pegawai Penerima Aset, Pegawai Pemeriksa Aset dan warga UMPSA |
| 2. Aset ICT yang diselenggara hendaklah merupakan milik UMPSA. Tanggungjawab yang perlu dipatuhi oleh pemilik aset ICT adalah | Pemilik Aset ICT dan warga UMPSA |

| | |
|---|---|
| termasuk perkara-perkara berikut:<br>a) Memastikan aset ICT di bawah tanggungjawabnya telah dimasukkan dalam senarai aset;<br>b) Memastikan aset ICT telah dikelaskan dan dilindungi;<br>c) Mengenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan;<br>d) Memastikan pengendalian aset ICT dilaksanakan dengan baik apabila aset dihapus atau dilupuskan;<br>e) Memastikan semua jenis aset dipelihara dengan baik;<br>f) Sebarang kehilangan/kecurian aset ICT adalah tertakluk kepada tatacara pengurusan aset UMPSA; dan<br>g) Sebarang kecurian maklumat adalah tertakluk kepada Prosedur Pengurusan Insiden Keselamatan ICT | |

| **5.10 MAKLUMAT PENGGUNAAN ASET YANG BOLEH DITERIMA YANG BERKAITAN *(ACCEPTABLE USE OF INFORMATION AND OTHER ASSOCIATED ASSETS)*** | |
|---|---|
| **PERNYATAAN POLISI** | **TANGUNGJAWAB** |
| 1. Peraturan atau kaedah penggunaan aset ICT yang dibenarkan yang mempunyai hubungkait dengan maklumat dan kemudahan memproses maklumat perlu dikenal pasti, didokumenkan dan dilaksanakan.<br><br>2. Mengenalpasti aset ICT dan maklumat yang boleh dan tidak boleh dikongsi;<br><br>3. Melaksanakan pemantauan terhadap aset ICT dan maklumat yang boleh dikongsi; | Warga UMPSA |

| | |
|---|---|
| 4. Aktiviti pengendalian maklumat di dalam aset ICT seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan melupus hendaklah mengambil kira langkah-langkah keselamatan berikut:<br>a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;<br>b) Memeriksa dan menentukan maklumat adalah tepat dan lengkap dari semasa ke semasa;<br>c) Menentukan maklumat sedia untuk digunakan;<br>d) Menjaga kerahsiaan kata laluan;<br>e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;dan<br><br>5. Prosedur penggunaan yang diterima harus disediakan mengikut klasifikasinya dan risiko yang ditentukan:<br>a) Menyediakan sekatan akses yang menyokong keperluan perlindungan untuk setiap tahap aktiviti;<br>b) Melaksanakan penyelenggaraan rekod pengguna yang dibenarkan untuk maklumat dan aset berkaitan;<br>c) Melaksanakan perlindungan salinan sementara atau kekal maklumat ke tahap yang konsisten dengan perlindungan maklumat asal;<br>d) Melaksanakan penyimpanan aset yang berkaitan dengan maklumat mengikut spesifikasi pengeluar;<br>e) Melaksanakan penandaan jelas semua salinan media penyimpanan (elektronik atau fizikal) untuk perhatian penerima yang dibenarkan; dan | |

| | |
|---|---|
| f) Mendapatkan kebenaran pelupusan maklumat dan aset berkaitan lain serta kaedah penghapusan yang disokong. | |

| **5.11 PEMULANGAN ASET *(RETURN OF ASSETS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Warga UMPSA hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan, penamatan perkhidmatan/kontrak atau aset ICT tersebut tidak digunakan lagi. | Warga UMPSA |

| **5.12 PENGELASAN MAKLUMAT *(CLASSIFICATION OF INFORMATION)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan dan garis panduan yang berkuatkuasa di UMPSA. | Pegawai Pengelas |

| **5.13 PELABELAN MAKLUMAT *(LABELLING OF INFORMATION)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan dan garis panduan yang berkuatkuasa di UMPSA.<br><br>Selain itu, panduan tentang tempat dan cara label boleh disediakan dengan mengenalpasti :<br>a) Tempat pelabelan;<br>b) Cara melabel maklumat yang dihantar atau yang disimpan; dan | Warga UMPSA |

| | |
|---|---|
| Cara mengendalikan kes di mana pelabelan tidak boleh dilakukan (contohnya disebabkan oleh sekatan teknikal) | |

| **5.14 PEMINDAHAN MAKLUMAT *(INFORMATION TRANSFER)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi;<br>b) Terma pemindahan data, maklumat dan perisian antara UMPSA dengan pihak luar hendaklah dimasukkan di dalam Perjanjian;<br>c) Media yang mengandungi maklumat perlu dilindungi; dan<br>d) Memastikan maklumat yang terdapat dalam mel elektronik hendaklah dilindungi sebaik-baiknya. | Pengguna, Warga UMPSA dan pembekal |
| 2. UMPSA perlu mengambil kira keselamatan maklumat dengan menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara UMPSA dengan pihak luar. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Pegawai yang bertanggungjawab hendaklah mengawal penghantaran dan penerimaan maklumat UMPSA;<br>b) Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat UMPSA; | CIO, ICTSO, Ketua Jabatan, Pengurus ICT, Pentadbir ICT, Pelaksana ICT dan Pemilik Aset ICT |

| | |
|---|---|
| c) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan<br>d) UMPSA hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data. | |
| 3. Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Pesanan elektronik merangkumi medium komunikasi digital termasuk tetapi tidak terhad kepada emel, *video conferencing* dan *cloud communication.* Perkara yang perlu dipatuhi dalam pengendalian pesanan elektronik perlu merujuk prosedur yang berkuat kuasa. | Warga UMPSA |
| 4. Perkara-perkara yang perlu dipatuhi dalam pengendalian komunikasi digital adalah seperti berikut :<br>a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh UMPSA sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;<br>b) Melindungi mesej daripada akses, pengubahsuaian atau penafian perkhidmatan yang tidak dibenarkan mengikut kategori klasifikasi yang diterima pakai oleh UMPSA;<br>c) Memastikan penggunaan alamat dan medium mesej yang betul; | Warga UMPSA |

| | |
|---|---|
| d) Kebolehpercayaan dan ketersediaan perkhidmatan;<br>e) Mempertimbangkan undang-undang yang boleh digunapakai, contohnya keperluan untuk tandatangan elektronik;<br>f) Mendapatkan kelulusan sebelum menggunakan perkhidmatan awam luaran seperti pemesejan segera *(instant messaging),* rangkaian sosial *(social networking)* atau perkongsian fail *(file sharing);* dan<br>g) Tahap pengesahan yang lebih kukuh untuk mengawal akses daripada rangkaian yang boleh diakses secara umum. | |

| **5.15 KAWALAN AKSES *(ACCESS CONTROL)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Prosedur kawalan capaian hendaklah diwujudkan, didokumenkan, dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini setahun sekali atau mengikut keperluan dan menyokong peraturan kawalan capaian sedia ada. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br>a) Keperluan keselamatan aset ICT dan rangkaian;<br>b) Hak akses dan dasar klasifikasi maklumat aset ICT dan rangkaian ;<br>c) Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa; | ICTSO, Pengurus ICT, Pentadbir ICT dan Pelaksana ICT |

| | |
|---|---|
| d) Kawalan akses ke atas perkhidmatan rangkaian dalaman dan luaran;<br>e) Menempatkan, mengasingkan atau memasang peralatan ICT yang bersesuaian untuk kawalan keselamatan antara rangkaian UMPSA, rangkaian agensi lain dan rangkaian awam;<br>f) Pengasingan peranan kawalan akses;<br>g) Kebenaran rasmi permintaan akses;<br>h) Keperluan semakan hak akses berkala melalui pemantauan dan penguatkuasaan kawalan akses pengguna terhadap aset ICT dan rangkaian ;<br>i) Pembatalan hak akses;<br>j) Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat;<br>k) Akses *privilege;*<br>l) Mewujud, menguatkuasakan dan memantau mekanisme untuk pengesahan pengguna, ID pengguna, kata laluan atau peralatan ICT yang dihubungkan ke rangkaian termasuk rangkaian tanpa wayar; dan<br>m) Kata nama pengguna yang diwujudkan perlu bersesuaian dengan nama sebenar pengguna dan di dalam bentuk yang rasmi; | |
| 2. Pengguna hendaklah menggunakan kemudahan rangkaian dengan cara yang bertanggungjawab. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:<br>a) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan | Pengguna |

| | |
|---|---|
| kesahihannya; laman web yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja, pembelajaran dan penyelidikan dan terhad untuk tujuan yang dibenarkan;<br><br>b) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan UMPSA;<br><br>c) Pengguna dilarang menyedia, memuat naik, memuat turun, menyimpan, mengguna dan menyebar maklumat atau bahan yang mempunyai unsur-unsur perjudian, keganasan, pornografi, fitnah, hasutan, perkara yang bercorak penentangan yang boleh membawa keadaan huru-hara serta maklumat yang menyalahi undang-undang;<br><br>d) Sebarang aktiviti memuat turun fail yang mempunyai *virus, spyware, worm,* dan sebagainya yang boleh mengancam keselamatan komputer dan rangkaian adalah dilarang sama sekali; dan<br><br>e) Pihak ICT UMPSA berhak menapis, menghalang dan mencegah penggunaan mana-mana laman web yang dianggap tidak sesuai merujuk kepada garis panduan yang berkuatkuasa. | |

| **5.16 PENGURUSAN IDENTITI *(IDENTITY MANAGEMENT)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Identiti digital mestilah mewakili seorang warga UMPSA yang boleh diletakkan kebertanggungjawaban ke atasnya. Ia merangkumi | Pengurus ICT, Pentadbir ICT, Pelaksana ICT, Pemilik Aset ICT, Warga |

| | |
|---|---|
| maklumat yang digunakan untuk mengenal pasti dan mengesahkan seseorang.<br><br>Proses pewujudan, pengaktifan, penyahaktifan, pengarkiban dan penghapusan identiti pengguna hendaklah dilaksanakan dan dipatuhi seperti berikut:<br>a) Akaun yang diperuntukkan oleh UMPSA sahaja boleh digunakan;<br>b) Akaun pengguna mestilah unik;<br>c) Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada pemilik aset ICT terlebih dahulu;<br>d) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;<br>e) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan mengikut prosedur yang sedang berkuatkuasa; dan<br>f) Identiti digital akan dinyahaktifkan jika individu yang dikaitkan dengan identiti digital tersebut telah meninggalkan organisasi atau bertukar peranan. Identiti digital tersebut seterusnya akan dihapuskan setelah 5 (LIMA) tahun dinyahaktifkan. | UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| **5.17 MAKLUMAT PENGESAHAN *(AUTHENTICATION INFORMATION)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan. | Pengguna, Pengurus ICT, Pentadbir ICT, Pelaksana ICT dan Pemilik Aset ICT |

| | |
|---|---|
| 2. Sistem pengurusan kata laluan hendaklah interaktif dan mengambilkira kualiti kata laluan yang dicipta. Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh UMPSA seperti yang berikut:<br>a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;<br>b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;<br>c) Panjang kata laluan mestilah sekurang kurangnya **DUA BELAS (12) AKSARA** dengan gabungan antara huruf, aksara khas dan nombor (alphanumeric) **KECUALI** bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad.<br>d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekali pun;<br>e) Kata laluan paparan kunci (lock screen) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;<br>f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara;<br>g) Kuat kuasakan pertukaran kata laluan semasa atau selepas login kali pertama atau selepas reset kata laluan;<br>h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;<br>i) Pengguna perlu mengikut amalan keselamatan yang baik di dalam | |

| | |
|---|---|
| pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti;<br>j) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum **TIGA (3) KALI** sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; dan<br>k) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.<br><br>3. Peranan dan tanggungjawab pengguna adalah seperti yang berikut:<br>a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber UMPSA;<br>b) Mengetahui dan memahami implikasi keselamatan siber dan kesan dari tindakannya;<br>c) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat UMPSA;<br>d) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;<br>e) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;<br>f) Menentukan maklumat sedia untuk digunakan;<br>g) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;<br>h) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran | |

| | |
|---|---|
| dan pemusnahan;<br>i) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.<br>j) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera; dan<br>k) Menghadiri program-program kesedaran mengenai keselamatan siber. | |

| **5.18 HAK AKSES *(ACCESS RIGHT)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Proses penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT perlu merujuk kepada prosedur yang berkaitan. | Pentadbir ICT, Pelaksana ICT, Warga UMPSA, Pemilik Aset ICT |
| 2. Pemilik Aset ICT hendaklah menyemak hak akses pengguna sekurang-kurangnya **1 TAHUN** sekali. Pemilik Aset ICT perlu mewujudkan Prosedur/SOP berkaitan Pendaftaran dan Penamatan Pengguna aset ICT masing- masing sebagai rujukan semakan ke atas hak akses pengguna mengikut masa yang ditetapkan. | Pengurus ICT, Pentadbir ICT, Pelaksana ICT dan Pemilik Aset ICT |
| 3. Hak akses warga UMPSA dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, pengajian, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam UMPSA. | ICTSO, Pengurus ICT, Pentadbir ICT, Pelaksana ICT, Pemilik Aset ICT dan Pengguna |

| **5.19 HUBUNGAN KESELAMATAN MAKLUMAT DENGAN PEMBEKAL *(INFORMATION SECURITY IN SUPPLIER RELATIONSHIP)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan | Pengurus ICT, Pentadbir ICT, Pelaksana ICT, |

| | |
|---|---|
| pembekal bagi mengurangkan risiko kepada aset UMPSA. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:<br>a) Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori di dalam sistem yang digunakan di UMPSA;<br>b) Proses pengurusan projek yang seragam untuk menguruskan pembekal berpandukan tatacara semasa yang berkuatkuasa;<br>c) Mengawal dan memantau akses pembekal sepanjang perlaksanaan projek;<br>d) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian;<br>e) Mematuhi kepada perjanjian, spesifikasi dan undang-undang yang telah dinyatakan;<br>f) Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber UMPSA kepada pembekal;<br>g) Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber UMPSA (Lampiran 2); dan<br>h) Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa. | Pemilik Projek, Pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| **5.20 PERJANJIAN KESELAMATAN MAKLUMAT DENGAN PEMBEKAL *(ADDRESSING INFORMATION SECURITY WITHIN SUPPLIER AGREEMENTS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat UMPSA. | Pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| | |
|---|---|
| Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak UMPSA selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.<br><br>Sekiranya pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak UMPSA mempunyai kuasa untuk menghalang pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi perlu merujuk kepada tatacara perolehan universiti yang sedang berkuatkuasa. | |

| **5.21 PENGURUSAN KESELAMATAN MAKLUMAT DALAM RANTAIAN KOMUNIKASI MAKLUMAT ICT *(MANAGING INFORMATION SECURITY IN THE INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SUPPLY CHAIN)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut:<br>a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan;<br>b) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan | Pengurus ICT, Pentadbir ICT, Pelaksana ICT, Pemilik Projek Pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| | |
|---|---|
| c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.<br><br>2. Pembekal produk ICT perlu menyebarkan amalan keselamatan yang sesuai di seluruh rantaian bekalan termasuk komponen yang dibeli atau diperoleh daripada pembekal lain atau entiti lain;<br><br>3. Melaksanakan proses pemantauan dan kaedah yang boleh diterima untuk mengesahkan produk dan perkhidmatan ICT yang disampaikan mematuhi keperluan keselamatan yang dinyatakan;<br><br>4. Memastikan jaminan, ketulenan produk dan perkhidmatan ICT boleh dikenalpasti serta menepati tahap keselamatan yang telah ditetapkan;<br><br>5. Mengenalpasti rantaian pembekalan bagi produk dan perkhidmatan ICT termasuk perkhimatan awan; dan<br><br>6. Mengurus kitaran hayat komponen ICT dan risiko keselamatan yang berkaitan. | |

| **5.22 PEMANTAUAN, SEMAKANSEMAKAN DAN PERUBAHAN PENGURUSAN PERKHIDMATAN PEMBEKAL *(MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. UMPSA hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: | Pengurus ICT, Pentadbir ICT, Pelaksana ICT, Pemilik Projek, Pembekal, pakar runding dan pihak |

| | |
|---|---|
| a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan;<br>b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan;<br>c) Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian;<br>d) Menjalankan proses audit kepada pembekal dan sub-pembekal;<br>e) Mengambil tindakan dan maklumbalas terhadap laporan audit; dan<br>f) Melaksanakan penilaian secara berkala bahawa pembekal mengekalkan tahap keselamatan maklumat yang mencukup<br><br>2. Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kepentingan maklumat, sistem dan proses perniagaan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti yang berikut:<br>a) Perubahan dalam perjanjian dengan pembekal;<br>b) Perubahan yang dilakukan oleh UMPSA bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan<br>c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk | yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| | |
|---|---|
| baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor. | |

| **5.23 KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN AWAN *(INFORMATION SECURITY FOR USE OF CLOUD SERVICES)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Perkhidmatan awan adalah penting untuk memastikan bahawa organisasi memilih penyedia perkhidmatan awam yang mempunyai tahap keselamatan yang tinggi. Berikut adalah beberapa langkah-langkah yang diperlukan sebelum penggunaan perkhidmatan awan.<br>a) Menetapkan skop perolehan perkhidmatan awan yang ingin dikawal. Skop ini perlu merangkumi jenis perkhidmatan awan yang diperlukan, data yang akan dipindahkan ke awan, dan syarat-syarat keselamatan yang dikehendaki;<br>b) Melakukan penilaian risiko untuk mengenal pasti potensi ancaman dan kerentanan yang berkaitan dengan penggunaan perkhidmatan awan. Ini memungkinkan anda untuk mengenal pasti tahap risiko dan mengambil tindakan untuk mengurangkan risiko tersebut;<br>c) Memilih penyedia perkhidmatan awan yang mematuhi piawaian keselamatan maklumat dan memiliki rekod prestasi yang baik dalam bidang keselamatan dan privasi data;<br>d) Membuat perjanjian perkhidmatan dengan penyedia perkhidmatan awan yang mencakupi butiran keselamatan | ICTSO, Pengurus ICT, Pentadbir ICT, Pelaksana ICT dan Pemilik Aset ICT |

| | |
|---|---|
| maklumat, seperti tahap layanan, perlindungan data, pematuhan piawaian, pemisahan data, pemulihan bencana, dan peraturan pematuhan;<br><br>e) Melakukan audit keselamatan secara berkala ke atas penyedia perkhidmatan awan untuk memastikan pematuhan mereka terhadap perjanjian perkhidmatan dan piawaian keselamatan maklumat;<br><br>f) Memastikan bahawa penyedia perkhidmatan awan mempunyai perancangan pemulihan bencana yang kukuh untuk melindungi data organisasi dalam kejadian insiden yang merugikan;<br><br>g) Menilai semula keselamatan maklumat secara berkala dan memastikan ia selaras dengan keperluan keselamatan dan piawaian; dan<br><br>h) Memastikan bahawa organisasi mematuhi peraturan, perundangan atau prosedur yang berkaitan dengan penggunaan perkhidmatan awan, terutamanya dalam hal privasi data dan perlindungan data peribadi. | |

| **5.24 PERANCANGAN, PENYEDIAAN DAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY INCIDENT MANAGEMENT PLANNING AND PREPARATION)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Tanggungjawab dan prosedur pengurusan insiden hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan | ICTSO, Pengurus ICT, UMPSA CSIRT, Pentadbir ICT, Pelaksana ICT dan Pemilik Aset ICT |

| | |
|---|---|
| insiden UMPSA adalah berdasarkan kepada Prosedur Pengurusan Pengendalian Insiden Keselamatan Siber UMPSA yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Memberikan kesedaran berkaitan Prosedur Pengendalian Insiden Keselamatan Siber UMPSA dan hebahan kepada warga UMPSA sekiranya ada perubahan; dan<br><br>b) Memastikan hanya personel yang bertauliah boleh mengurus insiden dan mempunyai tahap kompetensi yang diperlukan. | |

| **5.25 PENILAIAN DAN KEPUTUSAN PERISTIWA KESELAMATAN MAKLUMAT *(ASSESSMENT AND DECISION ON INFORMATION SECURITY EVENTS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat dengan merujuk kepada prosedur yang berkaitan. | ICTSO, UMPSA CSIRT dan Pelaksana ICT |

| **5.26 MAKLUMBALAS INSIDEN KESELAMATAN MAKLUMAT *(RESPONSE TO INFORMATION SECURITY INCIDENT)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Pengurusan Pengendalian Insiden Keselamatan Siber UMPSA. | ICTSO, UMPSA CSIRT dan Pelaksana ICT |

| | |
|---|---|
| Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut:<br>a) Mengenalpasti sistem yang terjejas kesan daripada insiden yang merebak;<br>b) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku;<br>c) Menghubungi pihak yang berkenaan dengan secepat mungkin;<br>d) Menyimpan jejak audit, salinan simpanan data secara berkala dan merekodkan semua bahan bukti;<br>e) Menjalankan kajian forensik sekiranya perlu;<br>f) Menyediakan pelan kontigensi, mengaktifkan pelan kesinambungan perkhidmatan dan pelan tindakan pemulihan dengan segera (jika perlu); dan<br>g) Mengenalpasti tindakan pengukuhan untuk mengatasi kelemahan keselamatan maklumat. | |

| **5.27 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT *(LEARNING FORM INFORMATION SECURITY INCIDENTS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Pengetahuan yang diperoleh daripada analisis dan penyelesaian insiden keselamatan maklumat perlu digunakan untuk mengurangkan kemungkinan insiden keselamatan maklumat berlaku pada masa hadapan atau mengurangkan kesannya.<br><br>Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah. | ICTSO, UMPSA CSIRT dan Pelaksana ICT |

| **5.28 PENGUMPULAN BUKTI *(COLLECTION OF EVIDENCE)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Pasukan UMPSA CSIRT perlu mendokumenkan dengan jelas bahan-bahan bukti seperti koleksi, pemerolehan dan pemeliharaan maklumat bagi insiden keselamatan maklumat yang diuruskan berdasarkan kepada Prosedur Pengurusan Pengendalian Insiden Keselamatan Siber UMPSA yang sedang berkuat kuasa. | ICTSO, UMPSA CSIRT dan Pelaksana ICT |

| **5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN *(INFORMATION SECURITY DURING DISRUPTION)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. UMPSA hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana.<br>Dalam merancang kesinambungan keselamatan maklumat, UMPSA perlu mengambil kira isu- isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi UMPSA.<br>UMPSA juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai.<br>Perkara yang perlu dipertimbangkan adalah seperti yang berikut:<br>a) Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) UMPSA;<br>b) Menetapkan polisi PKP;<br>c) Mengenal pasti perkhidmatan kritikal; | Koordinator PKP, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan Bencana ICT dan Pelaksana ICT |

| | |
|---|---|
| d) Melaksanakan Kajian Impak Perkhidmatan *(Business Impact Analysis — BIA)* untuk mengenalpasti fungsi kritikal perniagaan dalam membuat kesinambungan perkhidmatan berkaitan dengan ICT berdasarkan kepada Prosedur Operasi Standard: Pelan Pengurusan Kesinambungan Perkhidmatan yang sedang berkuat kuasa dan Penilaian Risiko terhadap perkhidmatan kritikal;<br>e) Membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT.<br>f) Melaksanakan program kesedaran dan latihan pasukan PKP dan warga UMPSA;<br><br>2. UMPSA hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:<br>a) Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal UMPSA yang telah dikenal pasti berdasarkan kepada Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT terkini;<br>b) Melaksanakan post-mortem dan mengemaskini pelan-pelan PKP; | |

| | |
|---|---|
| c) Mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal UMPSA;<br>d) Mengemas kini struktur tadbir urus PKP UMPSA jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan<br>e) Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP. | |
| 3. UMPSA hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan. | Pengurusan Atasan UMPSA, Koordinator PKP, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan Bencana ICT, Pemilik Perkhidmatan Kritikal UMPSA dalam PKP dan warga UMPSA |

| **5.30 KETERSEDIAAN ICT UNTUK KESINAMBUNGAN PERKHIDMATAN ICT *(ICT READINESS FOR BUSINESS CONTINUITY)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Teknologi Maklumat dan Komunikasi (ICT) adalah aspek penting dalam memastikan kesinambungan operasi organisasi. Ini melibatkan penyediaan infrastruktur, sistem, dan perkhidmatan ICT yang boleh diakses dan berfungsi dengan baik dalam semua keadaan, termasuk semasa krisis atau gangguan.<br>Faktor-faktor yang perlu dipertimbangkan untuk mencapai ketersediaan ICT bagi kesinambungan organisasi adalah seperti berikut :<br>a) Organisasi perlu mempunyai perancangan strategik ICT yang jelas dan | ICTSO, Pengurus ICT, Pentadbir ICT, Pelaksana ICT |

| | |
|---|---|
| menyeluruh yang mengenal pasti keperluan teknologi bagi menjayakan strategi kesinambungan perniagaan;<br>b) Organisasi perlu melaksanakan *Business Impact Analysis (BIA)* untuk mengenalpasti fungsi kritikal perniagaan dalam membuat kesinambungan perkhidmatan berkaitan dengan ICT;<br>c) Ini termasuk menentukan sumber daya ICT yang diperlukan, tujuan pemulihan, dan keupayaan perolehan peralatan dan perkhidmatan;<br>d) Mempunyai infrastruktur ICT yang *redundant*, termasuk rangkaian, pelayan, storan data, dan sokongan kuasa yang boleh berfungsi jika ada gangguan atau kegagalan;<br>e) Penggantian secara automatik *(failover)* dan peralatan cadangan perlu dipertimbangkan;<br>f) Lakukan pemantauan aktif terhadap peralatan ICT untuk mengenalpasti masalah sebelum ia berlaku dan mengelakkan gangguan;<br>g) Pengurusan inventori peralatan, pelan pembaikan, dan pemantauan prestasi berterusan;<br>h) Sediakan pelan pemulihan bencana ICT yang komprehensif. Ini termasuk cadangan data, pengekalkan cadangan pelayan, dan prosedur pemulihan semula aktiviti operasi UMPSA;<br>i) Ujian dan latihan berkala pelan pemulihan bencana;<br>j) Pastikan akses kepada sistem dan data dikawal dengan ketat dan disemak secara berkala. Ini termasuk pengurusan | |

| | |
|---|---|
| identiti, pengesahihan dua faktor, dan peraturan akses yang ketat;<br>k) Sediakan perkhidmatan pengurusan keselamatan seperti antivirus, *firewall,* dan pelindung kegagalan untuk menghalang ancaman keselamatan ICT;<br>l) Amalkan pemantauan keselamatan untuk mengenalpasti dan tindak balas kepada ancaman dan insiden keselamatan;<br>m) Pastikan staf tahu apa yang perlu dilakukan dalam kes insiden keselamatan;<br>n) Melaksanakan penyelenggaraan dan pembaikan peralatan dan sistem secara berkala untuk mengelakkan kegagalan yang tidak dijangka;<br>o) Tetapkan jadual pembaikan berkala dan pemulihan data;<br>p) Pantau penggunaan sumber daya ICT seperti *bandwidth* dan kapasiti penyimpanan untuk mengelakkan penggunaan berlebihan yang boleh menyebabkan gangguan; dan<br>q) Pastikan penyedia perkhidmatan awan atau penyedia perkhidmatan lain mempunyai pelan kesinambungan perniagaan yang mencukupi yang dapat menyokong operasi UMPSA jika berlaku gangguan. | |

| **5.31 UNDANG – UNDANG BERKANUN, PERATURAN DAN KEPERLUAN KONTRAK *(LEGAL, STATUTORY, REGULATORY AND CONRACTUAL REQUIREMENTS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Keperluan perundangan, berkanun dan kontraktual berkaitan dengan keselamatan maklumat dan | Warga UMPSA, pembekal, pakar runding |

| | |
|---|---|
| pendekatan UMPSA di dalam memenuhi keperluan tersebut hendaklah dikenal pasti, didokumenkan dan sentiasa dikemas kini. Undang-undang, peraturan dan dasar yang berkaitan dan perlu dipatuhi oleh semua pengguna di UMPSA dan pembekal adalah seperti di **Lampiran 1**. | dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| **5.32 HAK HARTA INTELEK *(INTELLECTUAL PROPERTY RIGHTS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Perlindungan hak harta intelek UMPSA hendaklah dilaksanakan mengikut undang-undang, peraturan dan prosedur yang berkaitan. | Warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| **5.33 PERLINDUNGAN REKOD *(PROTECTION OF RECORDS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, akses tanpa kebenaran dan pendedahan tanpa kebenaran. | Warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| **5.34 PRIVASI DAN PERLINDUNGAN MAKLUMAT PENGENALAN PERIBADI *(PRIVACY AND PROTECTION OF PERSONAL IDENTIFIABLE INFORMATION (PII)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| UMPSA hendaklah mengenal pasti dan memelihara keperluan berkenaan pemeliharaan dan perlindungan privasi mengikut undang-undang, peraturan dan tanggungjawab kontraktual yang berkuat kuasa. | Warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| **5.35 SEMAKAN BEBAS TERHADAP KESELAMATAN MAKLUMAT *(INDEPENDENT REVIEW OF INFORMATION SECURITY)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Pendekatan UMPSA dalam mengurus keselamatan maklumat dan pelaksanaannya termasuk manusia, proses dan teknologi perlu disemak secara bebas dan mengikut selang masa yang dirancang, atau apabila berlaku perubahan yang signifikan. | Warga UMPSA, Pelaksana ICT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| **5.36 PEMATUHAN POLISI, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT *(COMPLIANCE WITH POLICIES, RULES AND STANDARD FOR INFORMATION SECURITY)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Pematuhan kepada polisi, peraturan dan piawaian keselamatan maklumat hendaklah dipantau dan disemak secara berkala oleh UMPSA. | Pengurus ICT, Pentadbir ICT, Pelaksana ICT dan Pemilik Aset ICT |

| **5.37 PROSEDUR OPERASI YANG DIDOKUMENKAN *(DOCUMENTED OPERATING PROCEDURE)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Prosedur operasi terkini bagi kemudahan pemprosesan maklumat hendaklah didokumenkan, disimpan, dikawal dan disediakan kepada staf UMPSA mengikut proses yang terpakai di UMPSA. | Pengurus ICT, Pentadbir ICT, Pelaksana ICT dan Pemilik Aset ICT |

## 6 KAWALAN MANUSIA *(PEOPLE CONTROLS)*

### 6.1 PEMERIKSAAN *(SCREENING)*

| PERKARA | TANGUNGJAWAB |
|---|---|
| Tapisan keselamatan hendaklah dijalankan terhadap staf UMPSA yang terlibat selaras dengan keperluan perkhidmatan oleh PTJ yang berkaitan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Setiap proses tapisan yang dijalankan perlu dimaklumkan atau mendapat kebenaran daripada pemohon terlebih dahulu sebelum tapisan dijalankan; dan<br>b) Keperluan dalam membuat tapisan perlu dimasukkan di dalam terma kontrak di antara pemohon bagi memastikan bahawa setiap proses tapisan dijalankan mengikut kepada Akta Perlindungan Data Personal (PDPA) 2010. | Staf UMPSA dan PTJ yang berkaitan |

### 6.2 TERMA DAN SYARAT PEKERJAAN *(TERMS AND CONDITION EMPLOYMENT)*

| PERKARA | TANGUNGJAWAB |
|---|---|
| Persetujuan berkontrak dengan staf UMPSA hendaklah menyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut:<br>a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab staf UMPSA, yang terlibat dalam menjamin keselamatan aset ICT; dan<br>b) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa | Staf UMPSA dan PTJ yang berkaitan |

| | |
|---|---|
| berdasarkan perjanjian yang telah ditetapkan. | |

| **6.3 KESEDARAN KESELAMATAN MAKLUMAT, PENDIDIKAN DAN LATIHAN *(INFORMATION SECURITY AWARENESS AND TRAINING)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Warga UMPSA perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas- tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber UMPSA, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/system keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka;<br>b) Memastikan kesedaran yang berkaitan Polisi Keselamatan Siber UMPSA perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan<br>c) Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.; dan<br>d) Membuat penilaian terhadap kompetensi selepas diberi kesedaran berkaitan | ICTSO, Pelaksana ICT dan Warga UMPSA |

| | |
|---|---|
| Keselamatan ICT. | |

| **6.4 PROSES DISIPLIN *(DISCIPLINARY PROCESS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Proses tatatertib perlu dilaksanakan mengikut tatacara yang digariskan dalam undang- undang yang sedang berkuat kuasa di UMPSA. PTJ bertanggungjawab perlu memastikan:<br>a) Proses kerja tatatertib tersedia;<br>b) Seluruh warga UMPSA maklum serta mematuhi undang-undang yang terpakai di UMPSA;<br>c) Mana-mana pelanggaran terhadap peraturan tersebut boleh dikenakan tindakan tatatertib mengikut peruntukan undang-undang yang berkenaan; dan<br>d) Setiap maklumat berkaitan staf yang dikenakan tindakan tatatertib perlulah dilindungi selaras dengan prosedur yang berkenaan. | Unit Integriti, Jabatan Perundangan, Jabatan Pendaftar dan Jabatan Hal Ehwal Pelajar dan Alumni |

| **6.5 TANGGUNGJAWAB SELEPAS PENAMATAN ATAU PERUBAHAN PEKERJAAN (*RESPONSIBILITIES AFTER TERMINATION OR CHANGE OF EMPLOYMENT)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Warga UMPSA yang telah tamat perkhidmatan perlu mematuhi perkara-perkara berikut:<br>a) Warga UMPSA yang telah bertukar portfolio/fungsi tugas hendaklah memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada UMPSA mengikut tatacara yang telah ditetapkan;<br>b) Memastikan semua aset ICT UMPSA dikembalikan kepada UMPSA mengikut peraturan dan/atau terma yang | Jabatan Pendaftar, Jabatan Hal Ehwal Pelajar dan Alumni, Pelaksana ICT dan warga UMPSA |

| | |
|---|---|
| ditetapkan;<br><br>c) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan UMPSA dan/atau terma perkhidmatan yang ditetapkan;<br><br>d) Maklumat rasmi UMPSA dalam peranti tidak dibenarkan dibawa keluar dari UMPSA;<br><br>e) Menyedia dan menyerahkan nota serah tugas dan myPortfolio atau dokumen yang berkaitan kepada pegawai yang berkaitan; dan<br><br>f) Mengemaskini semua dokumentasi berkaitan pegawai yang tamat perkhidmatan bagi memastikan kesinambungan perkhidmatan UMPSA. | |

| **6.6 KERAHSIAAN ATAU PERJANJIAN KERAHSIAAN *(CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Keperluan universiti untuk melindungi maklumat perlulah dikenalpasti, dipatuhi, dipantau secara berkala, dan akujanji/perjanjian yang memperuntukkan tanggungjawab melindungi kerahsiaan maklumat hendaklah ditandatangani oleh staf UMPSA dan pihak - pihak yang berkepentingan.<br><br>Tanggungjawab kerahsiaan tersebut hendaklah dipersetujui dan dipatuhi oleh semua pihak bagi | ICTSO, Pengurus ICT, Pentadbir ICT, Pelaksana ICT, Pemilik Aset ICT, Pengguna dan Pembekal |

| | |
|---|---|
| memenuhi keperluan keselamatan maklumat yang relevan. | |

| **6.7 KERJA JARAK JAUH *(REMOTE WORKING)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja. Berikut adalah langkah-langkah yang perlu dipatuhi:<br>a) Memastikan proses pengesahan pengguna *remote* digunakan untuk mengawal capaian logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh;<br><br>b) Sebarang capaian ke dalam operasi teknikal oleh staf UMPSA dari luar UMPSA hanya dibenarkan dengan akses melalui VPN *(Virtual Private Network)* rasmi UMPSA dan perlu mendapat kelulusan Pengurus ICT yang berkaitan;<br><br>c) Pihak ketiga yang perlu melaksanakan kerja secara jarak jauh untuk memberi perkhidmatan sokongan atau bantuan teknikal hendaklah dipantau sepanjang masa sehingga tugas berkenaan selesai dengan menggunakan kaedah dan platform yang sesuai. Semua aktiviti capaian jarak jauh oleh pihak ketiga dan staf hendaklah direkod dan dipantau secara berterusan oleh pegawai yang bertanggungjawab terhadap tugasan berkaitan;<br><br>d) Sebarang perkara berkaitan pengurusan | Staf UMPSA,<br>Pihak ketiga, ICTSO,<br>Pengurus ICT dan<br>Pelaksana ICT |

| | |
|---|---|
| akaun VPN perlu merujuk kepada prosedur yang sedang berkuatkuasa; dan<br><br>e) Maklumat sensitif yang diproses dan disimpan di lokasi telekerja hendaklah dikendalikan dengan selamat dan semua dokumen fizikal mesti diuruskan mengikut tatacara pengurusan dokumen yang berkuatkuasa di UMPSA. | |

| **6.8 PELAPORAN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY EVENT REPORTING)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada UMPSA CSIRT yang kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:<br>a) Maklumat didapati hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa;<br><br>b) Maklumat disyaki hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa;<br><br>c) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;<br><br>d) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan;<br><br>e) Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau | ICTSO, UMPSA CSIRT, Pelaksana ICT, Warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| | |
|---|---|
| didedahkan;<br><br>f) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan<br><br>g) Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka.<br><br>2. Warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT serta mematuhi perkara-perkara berikut:<br>a) Kelemahan keselamatan maklumat mesti dilaporkan kepada UMPSA CSIRT dengan kadar segera bagi mengelakkan insiden keselamatan maklumat daripada berlaku;<br><br>b) Pengguna, kontraktor dan pihak ketiga adalah dilarang daripada membuktikan sebarang kelemahan sistem tanpa kebenaran; dan<br><br>c) Ujian untuk membuktikan kelemahan sistem tanpa kebenaran boleh ditafsirkan sebagai penyalahgunaan sistem dan boleh menyebabkan kerosakan kepada sistem maklumat atau perkhidmatan. Ini boleh mengakibatkan tindakan undang-undang bagi individu yang menjalankan ujian tersebut. | |

## 7 KAWALAN FIZIKAL *(PHYSICAL CONTROLS)*

### 7.1 PERIMETER KESELAMATAN FIZIKAL *(PHYSICAL SECURITY PERIMETERS)*

| PERKARA | TANGUNGJAWAB |
|---|---|
| Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan aset ICT UMPSA.<br><br>Perkara-perkara yang perlu dipatuhi termasuk yang berikut:<br>a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;<br><br>b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan warga UMPSA yang diberi kebenaran sahaja boleh melalui pintu masuk ini;<br><br>c) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;<br><br>d) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia;<br><br>e) Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk staf yang bekerja di dalam kawasan terhad; | Bahagian Keselamatan, PTJ |

| | |
|---|---|
| f) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan<br><br>g) Memasang alat penggera, kamera litar tertutup (CCTV), sistem kad akses dan seumpamanya dengan merujuk kepada garis panduan yang ditetapkan. | |

| **7.2 KEMASUKAN FIZIKAL *(PHYSICAL ENTRY)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis UMPSA. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Setiap warga UMPSA hendaklah mempamerkan pas pekerja dan pas pelajar sepanjang waktu bertugas;<br><br>b) Semua pas hendaklah dikembalikan kepada UMPSA apabila bertukar, tamat perkhidmatan atau bersara (jika perlu) dengan merujuk kepada tatacara semasa;<br><br>c) Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset ICT UMPSA;<br><br>d) Kontraktor mestilah mempunyai permit kerja atau pas pekerja untuk melaksanakan kerja di dalam UMPSA;<br><br>e) Kehilangan pas hendaklah dilaporkan segera kepada Bahagian Keselamatan; | Warga UMPSA, Bahagian Keselamatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| | |
|---|---|
| dan<br><br>f) Semua pelawat hendaklah mematuhi tatacara kemasukan yang sedang berkuatkuasa;<br><br>2. Penghantaran dan pemunggahan perlu dilakukan di kawasan yang telah ditetapkan bagi menjamin keselamatan. UMPSA hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran. | |

| **7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN *(SECURING OFFICES, ROOMS AND FACILITIES)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Kawasan tempat bekerja, bilik mesyuarat, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan CCTV, pusat data atau mana-mana ruang yang dirasakan memerlukan kawalan keselamatan perlu dihadkan daripada diakses tanpa kebenaran;<br><br>b) Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan<br><br>c) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan. | Warga UMPSA, PTJ yang berkaitan, pelaksana ICT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| **7.4 PEMANTAUAN KESELAMATAN FIZIKAL *(PHYSICAL SECURITY MONITORING)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Akses tanpa kebenaran ke kawasan fizikal terhad seperti bilik *server* dan bilik peralatan ICT boleh mengakibatkan kehilangan kerahsiaan, ketersediaan, integriti dan keselamatan aset maklumat. Berikut adalah kawalan yang boleh dilaksanakan:<br>a) Kamera CCTV;<br>b) Kad akses;<br>c) Pengawal keselamatan;<br>d) Penggera keselamatan untuk penceroboh; dan<br>e) Alat perisian untuk pengurusan keselamatan fizikal.<br><br>Premis dan kawasan persekitaran perlu pemantauan berterusan bagi mengelakkan akses tanpa kebenaran. | Warga UMPSA, Bahagian Keselamatan, Pelaksana ICT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| **7.5 PERLINDUNGAN FIZIKAL DAN ANCAMAN PERSEKITARAN *(PROTECTION AGAINST PHYSICAL AND ENVIRONMENTAL THREATS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. UMPSA perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana. | PTJ berkaitan dan pihak yang telibat |

| **7.6 BEKERJA DI KAWASAN YANG SELAMAT *(WORKING IN SECURE AREA)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga UMPSA yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis UMPSA termasuklah Pusat Data.<br><br>Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut:<br>a) Sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran;<br><br>b) Akses adalah terhad kepada warga UMPSA yang telah diberi kuasa sahaja dan dipantau pada setiap masa;<br><br>c) Pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) kamera atau lain-lain peralatan yang sesuai;<br><br>d) Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual;<br><br>e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; | Pengurus ICT, Pentadbir ICT, Pelaksana ICT, Pemilik Aset ICT dan Bahagian Keselamatan |

| | |
|---|---|
| f) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan;<br><br>g) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam;<br><br>h) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan;<br><br>i) Memperkukuh dinding dan siling; dan<br><br>j) Mengehadkan jalan keluar masuk. | |

| **7.7 DASAR MEJA KOSONG DAN SKRIN KOSONG *(CLEAR DESK AND CLEAR SCREEN)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.<br><br>Clear Desk dan Clear Screen bermaksud tidak meninggalkan dan mendedahkan bahan- bahan yang sensitif sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.<br><br>Langkah-langkah yang perlu diambil termasuklah seperti yang berikut:<br>a) Menggunakan kemudahan *screen saver password* atau *logout* apabila meninggalkan komputer;<br>b) Menyimpan bahan-bahan sensitif di | Warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| | |
|---|---|
| dalam laci atau kabinet fail yang berkunci;<br>c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat;<br>d) E-mel masuk dan keluar hendaklah dikawal; dan<br>e) Menghalang penggunaan tanpa kebenaran bagi peralatan seperti mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital. | |

| **7.8 LOKASI DAN PERLINDUNGAN PERALATAN *(EQUIPMENT SITTING AND PROTECTION)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Aset ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut:<br>a) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;<br>b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;<br>c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;<br>d) Pengguna dilarang membuat instalasi sebarang perisian tambahan yang boleh menyebabkan aset ICT gagal berfungsi;<br>e) Pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka | Warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| | |
|---|---|
| sentiasa aktif *(activated)* dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;<br>f) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna;<br>g) Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;<br>*h)* Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Gen-Set);<br>i) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan.<br>j) Peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci;<br>k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan *(air ventilation)* yang sesuai;<br>l) Peralatan ICT yang hendak dipinjam atau dibawa ke luar premis UMPSA, perlulah mendapat kelulusan oleh pegawai yang telah dipertanggungjawabkan dan direkodkan bagi tujuan pemulangan dan pemantauan;<br>m) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah | |

| | |
|---|---|
| dikendalikan mengikut prosedur yang berkuatkuasa;<br>n) Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;<br>o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pelaksana ICT;<br>p) *Server* bagi capaian umum perlu diletakkan di Pusat Data UMPSA dan tertakluk kepada prosedur yang berkuatkuasa;<br>q) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal;<br>r) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir ICT untuk dibaik pulih;<br>s) Setiap pengguna hendaklah melaporkan sebarang bentuk penyelewengan atau salah guna aset ICT kepada ICTSO;<br>t) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;<br>u) Pengguna dilarang sama sekali mengubah ***password administrator*** yang telah ditetapkan oleh pihak ICT; dan<br>v) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan UMPSA sahaja. | |

| **7.9 KESELAMATAN ASET DI LUAR PREMIS *(SECURITY OF ASSETS OFF-PREMISES)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis UMPSA seperti kehilangan, kerosakan atau kecurian. Peralatan yang dibawa keluar dari premis UMPSA adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Peralatan perlu dilindungi dan dikawal sepanjang masa;<br><br>b) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh UMPSA bagi membawa masuk/keluar peralatan;<br><br>c) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan merujuk kepada tatacara semasa.<br><br>d) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian;<br><br>e) Sebarang kehilangan/kecurian aset ICT adalah tertakluk kepada tatacara pengurusan aset UMPSA; dan<br><br>f) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan. | Warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| **7.10 MEDIA STORAN *(STORAGE MEDIA)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh UMPSA. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut :<br>a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;<br>b) Mengehadkan dan menentukan capaian media kepad pengguna yang dibenarkan sahaja;<br>c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;<br>d) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan<br>e) Menyimpan semua jenis media di tempat yang selamat.<br>f) Aplikasi *public cloud storage* hendaklah diputuskan dari talian selepas selesai penggunaannya. | Pelaksana ICT dan Pengguna |
| 2. Kaedah pelupusan media adalah seperti berikut:<br>a) Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh UMPSA; dan<br>b) Media yang mengandungi maklumat | Pelaksana ICT, warga UMPSA dan Jawatankuasa yang dilantik untuk pelupusan asset |

| | |
|---|---|
| terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa. | |
| 3. Media yang mengandungi maklumat perlu dilindungi supaya tidak diperolehi oleh orang yang tidak dibenarkan serta dilindungi daripada sebarang penyalahgunaan atau kerosakan semasa proses pemindahan atau pengangkutan. | Pelaksana ICT dan Pengguna |
| 4. Aset ICT tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut:<br>a) Peralatan ICT yang hendak dibawa keluar dari premis UMPSA untuk tujuan rasmi, perlulah mendapat kelulusan pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan<br>b) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan merujuk kepada tatacara semasa. | Pengguna, Pegawai Aset, Warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| **7.11 UTILITI SOKONGAN *(SUPPORTING UTILITIES)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan perlu diselenggara dari semasa ke semasa (sekurang- kurangnya setahun sekali). | Pelaksana ICT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| | |
|---|---|
| Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada aset ICT. Perkara yang perlu dipatuhi bagi menjamin keselamatan bekalan kuasa adalah seperti berikut:<br>a) Melindungi semua aset ICT dari kegagalan bekalan elektrik dan menyalurkan bekalan yang sesuai kepada aset ICT;<br>b) Menggunakan peralatan sokongan seperti Uninterruptable Power Supply (UPS) dan penjana (generator) bagi perkhidmatan kritikal seperti di pusat data supaya mendapat bekalan kuasa berterusan; dan<br>c) Menyemak dan menguji semua peralatan sokongan bekalan kuasa secara berjadual. | |

| **7.12 KESELAMATAN KABEL *(CABLING SECURITY)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan.<br>Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah- langkah keselamatan yang perlu diambil adalah seperti yang berikut:<br>a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;<br>b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;<br>c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan | Pelaksana ICT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| | |
|---|---|
| ancaman kerosakan dan *wire tapping*;<br>d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui talian *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat; dan<br>e) Mematuhi tatacara pemasangan pengkabelan yang ditetapkan oleh pihak UMPSA; dan<br>f) Kabel yang digunakan mestilah mempunyai pengesahan SIRIM ataupun yang setara. | |

| **7.13 PENYELENGGARAAN PERKAKASAN *(EQUIPMENT MAINTENANCE)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.<br>Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut:<br>a) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;<br>b) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;<br>c) Memastikan perkakasan hanya diselenggara oleh staf atau pihak yang dibenarkan sahaja;<br>d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; | Pemilik Aset ICT, Pelaksana ICT, Pembekal |

| | |
|---|---|
| e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan;<br>f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pemilik Aset ICT / Pelaksana ICT; dan<br>g) Penyelenggaraan Aset ICT perlu dilaksanakan secara berkala dan pelaksanaan hendaklah dikawal selia secara tahunan. | |

| **7.14 PELUPUSAN SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN *(SECURE DISPOSAL OR RE-USE OF EQUIPMENT)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti *(overwrite)* sebelum dilupuskan atau diguna semula. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh UMPSA dan ditempatkan di UMPSA.<br><br>Peralatan ICT yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan UMPSA. Langkah-langkah seperti yang berikut hendaklah diambil:<br>a) Bagi peralatan ICT yang akan dilupuskan sebelum dipindah-milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat;<br>b) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh | Pegawai Aset, Pelaksana ICT dan Staf UMPSA |

| | |
|---|---|
| dilupuskan atau sebaliknya;<br>c) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;<br>d) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;<br>e) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara- perkara seperti yang berikut:<br>i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi;<br>ii. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *CPU* seperti *RAM*, *Hardisk*, *Motherboard* dan sebagainya;<br>iii. Menyimpan dan memindahkan perkakasan luaran komputer seperti *AVR*, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian atau jabatan di UMPSA;<br>iv. Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; dan<br>v. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab UMPSA.<br>f) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada | |

| | |
|---|---|
| media storan kedua seperti *external hard disk* atau *thumbdrive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.<br>g) Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal; Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan;<br>h) Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan yang berkuat kuasa;<br>i) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan<br>j) Pegawai Aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT. | |

| 8 KAWALAN TEKNOLOGI *(TECHNOLOGICAL CONTROLS)* | |
|---|---|
| **8.1 PERANTI AKHIR PENGGUNA *(USER END POINT DEVICES)*** | |
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Meluluskan dasar, arahan, peraturan dan langkah keselamatan berkaitan penggunaan peranti mudah alih ICT kepada warga UMPSA. | JPICT |
| 2. Membangun serta menyebarkan dasar dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih. | Pengurus ICT, Pentadbir ICT, Pelaksana ICT |
| 3. Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut:<br>a) Tamatkan sesi aktif apabila selesai tugas;<br>b) *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan<br>c) Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan. | Warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |
| 4. BYOD *(Bring Your Own Device)* merupakan peranti mudah alih persendirian seperti telefon pintar, tablet dan komputer riba yang digunakan oleh pengguna untuk melaksanakan tugas rasmi. Pengguna BYOD hendaklah mematuhi keseluruhan Polisi Keselamatan Siber UMPSA, undang-undang dan ketetapan UMPSA.<br><br>Pengguna BYOD adalah dilarang daripada melakukan perkara-perkara berikut: | Warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| | |
|---|---|
| a) Menggunakan peranti untuk mengakses, menyimpan dan menyebarkan maklumat rasmi kepada pihak yang tidak dibenarkan;<br>b) Menggunakan peranti untuk tujuan peribadi yang boleh mengganggu produktiviti kerja;<br>c) Menjadikan peranti sebagai medium sandaran *(backup)* daripada komputer bagi menyimpan maklumat rasmi UMPSA;<br>d) Membuat rakaman, mengedar, menyalin audio dan video rasmi untuk tujuan peribadi;<br>e) Menjadikan peranti sebagai *access point* kepada aset ICT jabatan untuk capaian ke Internet yang menyebabkan pelanggaran kepada keselamatan ICT; dan<br>f) Mengabaikan keselamatan peranti dengan sengaja seperti peralatan mudah alih tidak disimpan di tempat yang selamat apabila tidak digunakan. | |

| **8.2 HAK AKSES ISTIMEWA *(PRIVILEGED ACCESS RIGHT)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal.<br><br>Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas merujuk kepada prosedur yang berkaitan.<br><br>Hak akses istimewa membolehkan UMPSA mengawal akses kepada infrastruktur, aplikasi, aset mereka dan mengekalkan integriti semua data dan sistem yang disimpan. UMPSA hendaklah: | ICTSO, Pengurus ICT, Pelaksana ICT, Pentadbir ICT, Pemilik Aset ICT, dan Pengguna |

| | |
|---|---|
| a) Mengenal pasti pengguna yang memerlukan hak akses istimewa untuk setiap sistem atau proses (contohnya, sistem operasi, sistem pengurusan;<br>b) Memberikan hak akses istimewa kepada pengguna mengikut keperluan berdasarkan peranan dan fungsi mereka serta dikhaskan untuk tugas kritikal sahaja;<br>c) Melaksanakan proses memberi hak akses istimewa mengikut proses yang jelas dan merekod semua hak istimewa yang diberikan; dan<br>d) Melaksanakan semakan berkala terhadap hak akses istimewa yang diberikan dengan mengambilkira had tempoh yang dibenarkan. | |

| **8.3 SEKATAN AKSES MAKLUMAT *(INFORMATION ACCESS RESTRICTION)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut prosedur kawalan capaian yang sedang berkuatkuasa.<br><br>Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut :<br>a) Tidak membenarkan akses kepada maklumat sensitif oleh identiti pengguna yang tidak dikenali;<br>b) Menyediakan mekanisme konfigurasi untuk mengawal akses kepada maklumat dalam sistem, aplikasi, dan perkhidmatan;<br>c) Mengawal data yang boleh diakses oleh pengguna tertentu;<br>d) Mengawal identiti atau kumpulan identiti yang mempunyai akses, seperti baca, | Pengurus ICT, Pentadbir ICT, Pelaksana ICT dan Pemilik Aset ICT |

| | |
|---|---|
| tulis, hapus, dan laksana; dan<br>e) Menyediakan kawalan akses fizikal ke kawasan terkawal. | |

| **8.4 AKSES KEPADA KOD SUMBER *(ACCESS TO SOURCE CODE)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut:<br>a) Log audit perlu dikekalkan kepada semua akses kepada kod sumber;<br>b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan<br>c) Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik UMPSA. | Pentadbir ICT,<br>Pelaksana ICT |

| **8.5 PENGESAHAN KESELAMATAN *(SECURE AUTHENTICATION)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Kawalan terhadap capaian sistem aplikasi perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan adalah seperti yang berikut:<br>a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan UMPSA;<br>b) Menjana amaran (*alert*) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem;<br>c) Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin;<br>d) Mewujudkan satu teknik pengesahan | Pentadbir ICT |

| | |
|---|---|
| yang bersesuaian bagi mengesahkan pengenalan diri pengguna;<br>e) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; dan<br>f) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem. | |

| **8.6 PENGURUSAN KAPASITI *(CAPACITY MANAGEMENT)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :<br>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; dan<br>b) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. | Pemilik Aset ICT, Pelaksana ICT |

| **8.7 PERLINDUNGAN TERHADAP PERISIAN *MALWARE (PROTECTION AGAINST MALWARE)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan *malware* hendaklah dilaksanakan dan digabungkan | Pelaksana ICT, Pengguna |

| | |
|---|---|
| dengan kesedaran pengguna terhadap serangan tersebut.<br><br>Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya adalah seperti berikut :<br>a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti Antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS), *Content filtering* dan *Web Application Firewall (WAF)* serta mengikut prosedur penggunaan yang betul dan selamat *(best practice)*;<br>b) Memasang dan menggunakan perisian antivirus dengan merujuk kepada prosedur yang berkuat kuasa;<br>c) Sekiranya perisian antivirus mempunyai pengurusan berpusat, penetapan polisi dan penyediaan laporan jika berlaku *virus outbreak* dalam rangkaian dapat dilaksanakan;<br>d) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya serta dilaksanakan secara berkala;<br>e) Mengemas kini antivirus dengan signature/*pattern* antivirus yang terkini;<br>f) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;<br>g) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; dan<br>h) 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. | |

| **8.8 PENGURUSAN KELEMAHAN TEKNIKAL *(MANAGEMENT OF TECHNICAL VULNERABILITIES)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah- langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem aplikasi dan operasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;<br>b) Menganalisis tahap risiko kerentanan; dan<br>c) Mengambil tindakan pengolahan dan kawalan risiko. | Pelaksana ICT, UMPSA CSIRT |
| 2. UMPSA hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan teknikal. | Pengurus ICT, Pentadbir ICT, Pelaksana ICT dan Pemilik Aset ICT |

| **8.9 PENGURUSAN KONFIGURASI *(CONFIGURATION MANAGEMENT)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |

| | |
|---|---|
| Pengurusan konfigurasi ialah bahagian penting dalam operasi pengurusan aset organisasi yang lebih luas. Konfigurasi adalah kunci dalam memastikan rangkaian bukan sahaja beroperasi sebagaimana mestinya, tetapi juga dalam melindungi peranti daripada perubahan yang tidak dibenarkan atau pindaan yang salah di pihak staf penyelenggaraan dan/atau vendor. Perkara-perkara berikut perlu dipatuhi bagi memastikan keselamatan maklumat adalah terjamin:<br><br>a) Cuba untuk menggunakan panduan khusus vendor dan/atau sumber terbuka yang tersedia secara umum tentang cara terbaik untuk mengkonfigurasi aset perkakasan dan perisian;<br>b) Memenuhi keperluan keselamatan minimum untuk peranti, aplikasi atau sistem yang sesuai untuknya;<br>c) Bekerja selaras dengan usaha keselamatan maklumat organisasi yang lebih luas, termasuk semua kawalan ISO yang berkaitan; dan<br>d) Disemak pada selang masa yang sesuai untuk memenuhi kemas kini sistem dan/atau perkakasan, atau sebarang ancaman keselamatan yang berlaku. | Pentadbir ICT dan Pelaksana ICT |

| **8.10 PEMADAMAN MAKLUMAT *(INFORMATION DELETION)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Organisasi harus sedar tentang kewajipan mereka untuk memadamkan data yang disimpan di mana – mana contohnya di *cloud*, komputer peribadi, pelayan dalaman, pemacu keras, dan pemacu USB apabila ia tidak lagi diperlukan dengan:<br>a) Pilih kaedah pemadaman yang sesuai yang mematuhi mana-mana undang- | Pelaksana ICT dan Warga UMPSA |

| | |
|---|---|
| undang atau peraturan sedia ada seperti polisi perekodan rekod awam di Arkib Negara. Pilihan termasuk pemadaman biasa, tulis ganti atau penghapusan dikodkan.<br>b) Rekodkan hasil penyingkiran untuk rujukan masa hadapan.<br>c) Pastikan bahawa, apabila menggunakan vendor pemadaman khusus, organisasi memperoleh bukti yang mencukupi (biasanya melalui dokumentasi) bahawa pemadaman telah dilakukan.<br>d) Organisasi harus menyatakan dengan tepat keperluan mereka apabila menggunakan vendor pihak ketiga, termasuk kaedah pemadaman dan jangka masa, dan harus menjamin bahawa aktiviti pemadaman dimasukkan dalam kontrak yang mengikat. | |

| **8.11 PENYAMARAN DATA *(DATA MASKING)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Apabila menggunakan salah satu daripada teknik ini, organisasi harus mempertimbangkan:<br>a) Tahap penyamaran dan/atau penyamaran yang diperlukan, berbanding dengan sifat data;<br>b) Cara data bertopeng sedang diakses;<br>c) Sebarang perjanjian mengikat yang menyekat penggunaan data untuk disembunyikan;<br>d) Mengekalkan data bertopeng berasingan daripada mana-mana jenis data lain, untuk mengelakkan subjek data dikenal pasti dengan mudah; dan<br>e) Meneliti data yang diterima, dan bagaimana ia telah diberikan kepada | Pelaksana ICT dan Pemilik Aset ICT |

| | |
|---|---|
| mana-mana sumber dalaman atau luaran. | |

| **8.12 PENCEGAHAN KEBOCORAN DATA *(DATA LEAKAGE PREVENTION)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Kebocoran data sukar untuk dihapuskan sepenuhnya. Walau bagaimanapun, untuk meminimumkan risiko yang unik untuk operasi UMPSA, organisasi harus:<br>a) Klasifikasikan data selaras dengan piawaian industri yang diiktiraf (PII, data komersial, maklumat produk), untuk menetapkan tahap risiko yang berbeza-beza di seluruh bahagian;<br>b) Memantau dengan teliti saluran data yang diketahui yang banyak digunakan dan terdedah kepada kebocoran (cth. e-mel, pemindahan fail dalaman dan luaran, peranti USB);<br>c) Hadkan keupayaan pengguna untuk menyalin dan menampal data (jika berkenaan) ke dan dari platform dan sistem tertentu;<br>d) Kebenaran daripada pemilik data sebelum sebarang pemindahan data dilaksanakan;<br>e) Pertimbangkan untuk mengurus atau menghalang pengguna daripada mengambil tangkapan skrin atau mengambil gambar monitor yang memaparkan jenis data yang dilindungi;<br>f) Sulitkan sandaran yang mengandungi maklumat sensitif;<br>g) Merangka langkah keselamatan pintu masuk dan langkah pencegahan kebocoran yang melindungi daripada | Pelaksana ICT dan Pemilik Aset ICT |

| | |
|---|---|
| faktor luaran seperti (tetapi tidak terhad kepada) pengintipan industri, sabotaj, gangguan komersial dan/atau kecurian IP; dan<br>h) Memastikan perisian *operating system* dan antivirus sentiasa dikemaskini. | |

| **8.13 SANDARAN MAKLUMAT *(INFORMATION BACKUP)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Salinan sandaran *(backup)* maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran *(backup)* yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran *(backup)* hendaklah dilakukan mengikut prosedur yang telah ditetapkan. Sandaran *(backup)* hendaklah direkodkan dan disimpan di *off site*. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Membuat *backup* keselamatan ke atas sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;<br>b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat;<br>c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana;<br>d) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan. Kekerapan sandaran bergantung pada tahap kritikal | Pelaksana ICT dan Pemilik Aset ICT |

| | |
|---|---|
| maklumat, dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi *backup*; dan<br>e) Merekod dan menyimpan salinan *backup* di lokasi yang bersesuaian dan selamat. | |

| **8.14 KEMUDAHAN PEMPROSESAN MAKLUMAT YANG BERTINDIH *(REDUNDANCY OF INFORMATION PROCESSING FACILITIES)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Kemudahan pemprosesan maklumat UMPSA perlu mempunyai lewahan *(redundancy)* untuk infrastruktur ICT yang kritikal. Antara infrastruktur ICT di persekitaran UMPSA yang mempunyai lewahan *(redundancy)* adalah perkakasan rangkaian *(core switch, firewall),* perkakasan pusat data (server kritikal) serta fasiliti sokongan bekalan kuasa *(UPS dan generator set)* dan pendingin hawa di pusat data.<br><br>Kemudahan lewahan *(redundancy)* yang disediakan ini akan diuji dari aspek *failover test* secara berjadual sekali setahun dan dilaporkan hasil pengujiannya di dalam mesyuarat yang berkaitan dengan infrastruktur ICT UMPSA. | Koordinator Pelan Pemulihan Bencana ICT |

| **8.15 LOGGING *(LOGGING)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak | Pelaksana ICT |

| | | |
|---|---|---|
| | dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan.<br><br>Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh UMPSA. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti yang berikut:<br>a) fail log sistem pengoperasian;<br>b) fail log servis (web, e-mel);<br>c) fail log aplikasi (*audit trail*); dan<br>d) fail log rangkaian (*core switch, firewall*)<br><br>Pelaksana ICT hendaklah melaksanakan perkara - perkara berikut :<br>a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;<br>b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan<br>c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pelaksana ICT hendaklah melaporkan kepada UMPSA CSIRT. | |
| 2. | Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin. | Pelaksana ICT |
| 3. | Aktiviti Pelaksana ICT dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara tetap.<br>a) Memantau penggunaan kemudahan memproses maklumat secara berkala; | Pelaksana ICT, Pemilik Aset ICT dan UMPSA CSIRT |

| | |
|---|---|
| b) Aktiviti pelaksana ICT dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu;<br>c) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;<br>d) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan<br>e) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pelaksana ICT dan Pemilik Aset ICT hendaklah melaporkan kepada pasukan UMPSA CSIRT. | |

| **8.16 AKTIVITI PEMANTAUAN *(MONITORING ACTIVITIES)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Organisasi hendaklah memasukkan perkara berikut dalam operasi pemantauan mereka:<br>a) Kedua-dua trafik rangkaian masuk dan keluar, termasuk data ke, dan dari aplikasi;<br>b) Akses kepada platform kritikal organisasi, termasuk (tetapi tidak terhad kepada Sistem,*server*, Perkakasan rangkaian);<br>c) Sistem pemantauan itu sendiri;<br>d) Fail konfigurasi;<br>e) Log peristiwa daripada peralatan keselamatan dan platform perisian;<br>f) Semakan kod yang memastikan mana-mana program boleh digunakan adalah | Pelaksana ICT |

| | |
|---|---|
| dibenarkan dan bebas daripada ancaman;<br>g) Pengiraan, penyimpanan dan penggunaan sumber rangkaian dibuat jika penggunaan melebihi had yang ditetapkan;<br>h) Kaedah pemantauan juga perlu termasuk penjanaan laporan dan memberi amaran awal untuk menangani ancaman dengan segera; dan<br>i) Mengimplementasikan sistem penyimpanan rekod log yang teratur dengan tempoh penyimpanan yang jelas untuk membantu dalam audit dan penyiasatan insiden keselamatan. | |

| **8.17 PENYERAGAMAN JAM *(CLOCK SYNCHRONISATION)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal.<br><br>Waktu server dan peralatan ICT yang berpusat dan kritikal perlu diselaraskan dengan satu sumber waktu yang piawai menggunakan Network Time Protocol (NTP) Server.<br><br>Penyelarasan jam yang betul adalah penting untuk memastikan integriti data, keselamatan sistem, dan operasi yang efisien dalam pelbagai aplikasi, termasuk sistem pemprosesan maklumat.<br><br>Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam UMPSA atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang | Pelaksana ICT |

| | |
|---|---|
| ditetapkan oleh *National Metrology Institute of Malaysia* (NMIM). | |

| **8.18 KEISTIMEWAAN PENGGUNAAN UITILITI PROGRAM *(USE OF PRIVILEGED UTILITY PROGRAMS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *Over-Riding* sistem.<br>Untuk mengekalkan integriti rangkaian dan meningkatkan kesinambungan perkhidmatan, UMPSA hendaklah:<br>a) Menghadkan penggunaan program utiliti kepada staf pelaksana ICT secara khusus yang perlu menjalankan peranan kerja mereka;<br>b) Pastikan semua program utiliti dikenal pasti, disahkan dan dibenarkan selaras dengan keperluan perkhidmatan, dan pihak pengurusan dapat memperoleh pandangan atas bawah penggunaannya pada bila-bila masa;<br>c) Kenal pasti semua staf yang menggunakan program utiliti, sama ada sebagai sebahagian daripada tugas harian mereka, atau secara ad-hoc;<br>d) Laksanakan kawalan kebenaran yang mencukupi untuk mana- mana staf yang perlu menggunakan program utiliti, sama ada sebagai sebahagian daripada tugas harian mereka atau secara ad-hoc;<br>e) Menghalang penggunaan program utiliti pada mana-mana sistem yang dianggap perlu oleh organisasi untuk mengasingkan tugas;<br>f) Melaksanakan audit berkala terhadap penggunaan program utiliti dan menyediakan pemantauan berterusan | ICTSO, Pengurus ICT, Pentadbir ICT dan Pelaksana ICT |

| | |
|---|---|
| untuk mengesan aktiviti yang mencurigakan;<br>g) Program utiliti partition berbeza daripada aplikasi standard yang digunakan oleh perniagaan secara tetap, termasuk trafik rangkaian;<br>h) Hadkan ketersediaan program utiliti, dan gunakannya untuk tujuan nyata Sahaja;<br>i) Merekod log penggunaan program utiliti merangkumi masa dan pengguna yang dibenarkan; dan<br>j) Meningkatkan prosedur pengesahan untuk program utiliti dengan menggunakan pelbagai faktor pengesahan (multi-factor authentication) untuk meningkatkan keselamatan. | |

| **8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI *(INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti yang berikut:<br>a) Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian;<br>b) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; dan<br>c) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur. | Pengurus ICT, Pentadbir ICT dan Pelaksana ICT |
| 2. Peraturan yang mengawal pemasangan | Pelaksana ICT, warga |

| | |
|---|---|
| perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA.<br>b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;<br>c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; dan<br>d) Pentadbir ICT berhak menyekat mana-mana perisian yang dianggap tidak sesuai merujuk kepada garis panduan yang berkuatkuasa. | UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA |

| **8.20 KESELAMATAN RANGKAIAN *(NETWORKS SECURITY)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br>a) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; dan setiap konfigurasi perlu didokumentasi;<br>b) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas | ICTSO, Pengurus ICT, Pentadbir ICT, Pelaksana ICT, Pengguna |

| | |
|---|---|
| dari risiko seperti banjir, gegaran dan habuk;<br>c) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja;<br>d) Pengguna selain staf dan pelajar yang hendak menggunakan kemudahan rangkaian UMPSA hendaklah mengikut tatacara semasa yang berkuatkuasa;<br>e) *Firewall* hendaklah dipasang, dikonfigurasi, diselia dan diuruskan oleh Pentadbir ICT dan Pelaksana ICT;<br>f) Semua trafik keluar dan masuk rangkaian hendaklah melalui *firewall* di bawah kawalan UMPSA;<br>g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna KECUALI mendapat kebenaran daripada Pegawai Keselamatan Teknologi Maklumat (ICTSO);<br>h) Mempertimbangkan pemasangan perisian untuk menyekat aktiviti yang dilarang bagi mencegah sebarang cubaan pencerobohan serta aktiviti-aktiviti lain yang boleh mengancam data dan maklumat UMPSA;<br>i) Sebarang penyambungan rangkaian yang bukan di bawah kawalan DiTec UMPSA adalah tidak dibenarkan;<br>j) Pemasangan dan pengoperasian perkakasan rangkaian *(wired LAN* dan *wireless LAN)* yang bukan di bawah kawalan UMPSA adalah tidak dibenarkan kecuali keperluan untuk Pengajaran dan Pembelajaran (P&P) serta Penyelidikan & Pembangunan | |

| | |
|---|---|
| (R&D) hendaklah mendapat sokongan Ketua Jabatan dan kelulusan daripada ICTSO;<br>k) Kemudahan bagi *wireless LAN* hendaklah dipantau dan dikawal penggunaannya;<br>l) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance (SLA)* yang telah ditetapkan;<br>m) Memasang dan mengawal antara muka *(interfaces)* yang bersesuaian di antara rangkaian UMPSA, rangkaian agensi lain dan rangkaian awam;<br>n) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;<br>o) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja;<br>p) Mewujud dan melaksana kawalan pengalihan laluan *(routing control)* bagi memastikan pematuhan terhadap peraturan UMPSA. | |

| **8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN *(SECURITY OF NETWORK SERVICES)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Pengurusan bagi semua perkhidmatan rangkaian (*inhouse atau outsource*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian. | ICTSO,<br>Pengurus ICT,<br>Pentadbir ICT,<br>Pelaksana ICT dan<br>Pembekal |

| **8.22 PENGASINGAN RANGKAIAN *(SEGREGATION OF NETWORKS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian UMPSA. | Pengurus ICT, Pentadbir ICT dan Pelaksana ICT |

| **8.23 TAPISAN LAMAN WEB *(WEB FILTERING)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Organisasi harus mewujudkan dan melaksanakan kawalan yang diperlukan untuk menghalang warga UMPSA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT UMPSA daripada mengakses laman web yang mungkin mengandungi virus, bahan yang tidak selamat data atau jenis maklumat haram yang lain. Organisasi harus mempertimbangkan untuk menyekat akses kepada jenis laman web bagi kategori berikut:<br><br>a) Laman web dengan fungsi muat naik maklumat. Akses hendaklah tertakluk kepada kebenaran dan hanya boleh diberikan atas sebab yang sah atau mengikut mana-mana peraturan semasa;<br><br>b) Laman web yang diketahui atau disyaki mengandungi bahan berniat jahat, seperti laman web dengan kandungan perisian yang tidak selamat;<br><br>c) Pelayan perintah dan kawalan *(command and control servers)*;<br>d) Laman web berniat jahat *(malicious website);* dan<br>e) Laman web yang mengedarkan | ICTSO, Pengurus ICT, Pentadbir ICT, Pelaksana ICT |

| | |
|---|---|
| kandungan dan bahan yang menyalahi undang-undang. | |

| **8.24 PENGGUNAAN KRIPTOGRAFI *(USE OF CRYPTOGRAPHY)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Kriptografi merangkumi kaedah-kaedah seperti yang berikut:<br>a) Enkripsi - Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (*encryption*).<br>b) Tandatangan Digital - Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. | Pengurus ICT, Pentadbir ICT, Pelaksana ICT |

| **8.25 KITARAN HIDUP PEMBANGUNAN SELAMAT *(SECURE DEVELOPMENT LIFE CYCLE)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:<br>a) Keselamatan persekitaran pembangunan;<br>b) Keselamatan pangkalan data;<br>c) Keperluan keselamatan dalam spesifikasi dan fasa reka bentuk;<br>d) Keperluan *check point* keselamatan dalam pelaksanaan projek;<br>e) Keperluan pengetahuan ke atas keselamatan aplikasi serta latihan yang berkaitan;<br>f) Keselamatan repositori dan kawalan versi kod sumber; dan<br>g) Ujian sistem dan keselamatan, seperti imbasan kod dan ujian penembusan | Pengurus ICT, Pentadbir ICT dan Pelaksana ICT |

| | |
|---|---|
| Bagi pembangunan secara penyumberluaran (*outsource*), pembekal yang dilantik perlu berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem. | |

| **8.26 KEPERLUAN KESELAMATAN PERMOHONAN *(APPLICATION SECURITY REQUIREMENTS)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Perkara yang perlu dipertimbangkan adalah seperti berikut:<br><br>a) Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi UMPSA. Contoh perkhidmatan sumber luaran ialah:<br>i. Perisian Sebagai Satu Perkhidmatan;<br>ii. Platform Sebagai Satu Perkhidmatan;<br>iii. Infrastruktur Sebagai Satu Perkhidmatan;<br>iv. Storan Pengkomputeran Awan; dan<br>v. Pemantauan Keselamatan.<br>b) Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala;<br>c) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*);<br>d) Proses berkaitan dengan pihak yang | ICTSO, Pengurus ICT Pentadbir ICT, Pelaksana ICT Pengguna, dan Pemilik Aset ICT |

| | | |
|---|---|---|
| | berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi;<br>e) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan<br>f) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak. | |
| 2. | Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:<br>a) Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi;<br>b) Memastikan semua aspek transaksi dipatuhi:<br>i. maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan;<br>ii. mengekalkan kerahsiaan maklumat<br>iii. mengekalkan privasi pihak yang terlibat; dan<br>iv. protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi.<br>c) Pihak yang mengeluarkan tandatangan digital yang diiktiraf oleh Kerajaan. | ICTSO, Pengurus ICT Pentadbir ICT, Pelaksana ICT Pengguna, dan Pemilik Aset ICT |

| **8.27 SENIBINA SISTEM SELAMAT DAN PRINSIP KEJURUTERAAN *(SECURE SYSTEM ARCHITECTURES AND ENGINEERING PRINCIPLES)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Prinsip kejuruteraan keselamatan hendaklah disediakan, didokumentasikan, dan dilaksanakan dalam aktiviti kejuruteraan sistem maklumat.<br><br>Keselamatan perlu direka bentuk ke dalam semua lapisan *system architecture*.<br><br>Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada prosedur atau garis panduan yang berkuatkuasa. | Pengurus ICT, Pentadbir ICT dan Pelaksana ICT |

| **8.28 PENGEKODAN SELAMAT *(SECURE CODING)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Amalan dan prosedur pengekodan yang selamat hendaklah mengambil kira perkara berikut untuk proses pengekodan:<br>a) Prinsip pengekodan perisian yang selamat harus disesuaikan dengan setiap bahasa pengaturcaraan dan teknik yang digunakan;<br>b) Penggunaan teknik dan kaedah pengaturcaraan selamat seperti pembangunan yang hendak dilakukan hendaklah dibuat pengujian;<br>c) Penggunaan kaedah pengaturcaraan yang berstruktur;<br>d) Dokumentasi kod yang betul dan penyingkiran kecacatan kod;<br>e) Larangan ke atas penggunaan kaedah pengekodan perisian yang tidak selamat seperti sampel kod yang tidak | Pengurus ICT, Pentadbir ICT dan Pelaksana ICT |

| | |
|---|---|
| diluluskan atau kata laluan berkod keras *(hardcode)*; dan<br>f) Kod yang digunakan hendaklah sentiasa dikemaskini mengikut keadaan keselamatan semasa. | |

| **8.29 UJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN *(SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Menyemak dan mengesahkan input bagi menjamin proses dan ketepatan maklumat;<br>b) Memastikan fungsi aplikasi berjalan dengan betul dan sempurna;<br>c) Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; dan<br>d) Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.<br>Maklumat lanjut berkaitan pengujian keselamatan sistem boleh merujuk kepada dokumen **ISO/IEC/IEEE 29119 *Software Testing Standard*.** | Pelaksana ICT, Pemilik Aset ICT dan Pengguna |
| 2. Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Pengujian penerimaan sistem hendaklah merangkumi Keperluan Keselamatan Sistem Maklumat dan | PentadbirICT, Pelaksana ICT, Pemilik Aset ICT dan Pengguna |

| | |
|---|---|
| kepatuhan kepada prosedur yang sedang berkuatkuasa;<br>b) Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai; dan<br>c) Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan *(vulnerability scanner*).<br>Maklumat lanjut berkaitan boleh merujuk kepada dokumen **ISO/IEC/IEEE 29119** Software Testing Standard. | |

| **8.30 PEMBANGUNAN SUMBER LUAR *(OUTSOURCED DEVELOPMENT)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| UMPSA hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Bagi sistem aplikasi yang dibangunkan oleh pembekal, klausa mengenai pemindahan Teknologi *(Transfer of Technology)*, tempoh jaminan dan kod *sumber (source code)* hendaklah dinyatakan dengan jelas dalam dokumen perjanjian. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Pelesenan, pemilikan kod, dan hak harta intelek yang berkaitan dengan pembangunan sistem*;*<br>b) Bagi semua perkhidmatan sumber luaran, spesifikasi perolehan dan terma perjanjian hendaklah menyatakan bahawa kod sumber adalah **HAK MILIK UMPSA** sepenuhnya dan perlu diserahkan kepada UMPSA;<br>c) Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian | ICTSO, Pengurus ICT, Pentadbir ICT, Pelaksana ICT, Pemilik Aset ICT |

| | |
|---|---|
| pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik;<br>d) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem;<br>e) Mengguna pakai prinsip dan tatacara *escrow* (sekiranya perlu*);* dan<br>f) Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian. | |

| **8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PENGELUARAN *(SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENT)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem.<br><br>1. UMPSA perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira perkara-perkara berikut:<br>a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem;<br>b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran;<br>c) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem;<br>d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem;<br>e) Pegawai yang bekerja di dalam | Pengurus ICT, Pentadbir ICT dan Pelaksana ICT |

| | |
|---|---|
| persekitaran pembangunan sistem ialah yang boleh dipercayai; dan<br>f) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.<br><br>2. Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran *(production)*.<br>b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan<br>c) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat. | |

| **8.32 PENGURUSAN PERUBAHAN *(CHANGE MANAGEMENT)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| 1. Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br>a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat | Pengurus ICT,Pentadbir ICT, Pelaksana ICT, Pemilik Aset ICT |

| | | |
|---|---|---|
| | kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;<br>b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;<br>c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan;<br>d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja; dan<br>e) Semua aktiviti yang melibatkan perubahan perlu merujuk kepada prosedur yang sedang berkuatkuasa. | |
| 2. | Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem hendaklah dikawal. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :<br>a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;<br>b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk | Pengurus ICT,Pentadbir ICT, Pelaksana ICT, Pemilik Aset ICT |

| | | |
|---|---|---|
| | terhadap operasi dan keselamatan UMPSA. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan;<br>c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;<br>d) Keperluan dan kesesuaian perubahan terhadap sistem pengoperasian dan perisian sokongan perlu dikaji terlebih dahulu;<br>e) Sebarang perubahan sistem pengoperasian dan perisian sokongan perlu diuji dahulu di dalam *development server* sebelum dimuatnaik di dalam *production server;*<br>f) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pelaksana ICT yang dibenarkan; dan<br>g) Menghalang sebarang peluang untuk kebocoran maklumat. | |
| 3. | Apabila platform operasi berubah, aplikasi utama UMPSA hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan organisasi. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform;<br>b) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan | Pentadbir ICT, Pelaksana ICT, Pemilik Aset ICT |

| | |
|---|---|
| c) Memastikan perubahan yang sesuai dibuat kepada Pelan Kesinambungan Perkhidmatan (PKP) UMPSA dan Pelan Pemulihan Bencana (DRP) yang berkaitan. | |
| 4. Pengubahsuaian ke atas pakej perisian adalah terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal mengikut prosedur yang sedang berkuatkuasa. | Pelaksana ICT |
| 5. Penggunaan *Versioning Control Software* (VCS) di dalam pembangunan dan penyelenggaraan sistem bagi memastikan terdapat kawalan perubahan pada pakej sistem. | Pelaksana ICT |

| **8.33 MAKLUMAT UJIAN *(TEST INFORMATION)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian;<br>b) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian;<br>c) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan<br>d) Merekodkan sebarang penyalinan dan penggunaan data sebenar. | Pentadbir ICT, Pelaksana ICT, Pemilik Aset ICT dan Pengguna |

| **8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PENGUJIAN AUDIT** ***(PROTECTION OF INFORMATION SYSTEMS DURING AUDIT TESTING)*** | |
|---|---|
| **PERKARA** | **TANGUNGJAWAB** |
| Keperluan dan aktiviti audit yang melibatkan penentusahan atau pengujian sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses operasi organisasi. | Pentadbir ICT, Pelaksana ICT, Pemilik Aset ICT dan Pengguna |

**LAMPIRAN 1**

## UNDANG – UNDANG, PERATURAN DAN DASAR YANG TERPAKAI

Polisi Keselamatan Siber UMPSA ini hendaklah dibaca bersama dengan akta-akta, warta, pekeliling-pekeliling, surat pekeliling dan peraturan dalaman yang berkaitan dan sedang berkuatkuasa antaranya seperti berikut;

**i. Akta dan Arahan :**

a) Arahan Keselamatan;
b) Akta Komunikasi dan Multimedia 1998 [Akta 588];
c) Akta Tandatangan Digital 1997 [Akta 562];
d) Akta Jenayah Komputer 1997 9 [Akta 563];
e) Akta Hak Cipta 1987 [Akta 332];
f) Akta Rahsia Rasmi 1972 [Akta 88];
g) Arahan Perbendaharaan;
h) Akta Cap Dagangan 2019 [Akta 815];
i) Akta Keselamatan Siber 2024 [Akta 854];
j) Perlembagaan Universiti Malaysia Pahang Al-Sultan Abdullah [P.U. (A) 464/2010];
k) Kaedah-Kaedah Universiti dan Kolej Universiti (Universiti Malaysia Pahang Al-Sultan Abdullah) (Tatatertib Pelajar) 2024 [P.U. (A) 322/2024]
l) Akta Universiti dan Kolej Universiti 1971 [Akta 30]
m) Arahan Teknologi Maklumat 2007;
n) Akta Badan Berkanun (Tatatertib & Surcaj) 2000 [Akta 605];
o) Akta Aktiviti Kerajaan Elektronik 2007 [Akta 680];
p) Akta Perlindungan Data Peribadi 2010 [Akta 709];
q) Akta Teleperubatan 1997 [Akta 564];
r) Akta Suruhanjaya Komunikasi dan Multimedia Malaysia 1998 [Akta 589]; dan
s) Akta Bekalan Elektrik 1990 [Akta 447]

**ii. Pekeliling Am :**

a) Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
b) Malaysian Public Sector *Management of Information and Communications Technology Security Handbook (MyMIS)* 2002;

c) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) yang dikeluarkan oleh MAMPU;
d) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan;
e) Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 – Tatacara Pengurusan Aset Alih Kerajaan (TPA);
f) Pekeliling Am Bil. 6 Tahun 1999: Garis Panduan Pelaksanaan Perkongsian Pintar Antara Agensi-agensi Kerajaan Dalam Bidang Teknologi Maklumat yang dikeluarkan oleh MAMPU;
g) Pekeliling Am Bil. 3 Tahun 2000: Dasar Keselamatan ICT Kerajaan yang dikeluarkan oleh MAMPU;
h) Pekeliling Am Bil.1 Tahun 2000: Garis Panduan *Malaysian Civil Service Link (MCSL)* dan Laman Web Kerajaan yang dikeluarkan oleh MAMPU;
i) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021: Dasar Perkhidmatan Pengkomputeran Awan Sekto Awam;
j) Pelupusan Rekod Awam: Arkib Negara (Jadual Pelupusan Rekod Urusan Am dan Jadual Pelupusan Rekod Kewangan dan Perakaunan 2023); dan
k) Pekeliling Am Bil.4 Tahun 2022: Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam.

**iii. Surat Arahan KP (Ketua Pengarah MAMPU) :**

a) Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan yang bertarikh 1 Jun 2007;
b) Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Pemantapan Pelaksanaan Sistem Mel Elektronik D Agensi-agensi Kerajaan yang bertarikh 23 November 2007;
c) Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;
d) Surat Arahan UMP.702-1/1/7 Jld. 3 (48) bertarikh 23 Mac 2009 bertajuk “Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-agensi Kerajaan”;

e) Surat Arahan UMP.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk “Penggunaan Media Jaringan Sosial di Sektor Awam”; dan

f) Surat Arahan Ketua Pengarah UMP bertarikh 1 Jun 2007 “Langkah-langkah mengenai penggunaan Mel Elektronik Agensi – Agensi Kerajaan”, Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan Government Unified Communication (MyGovUC).

**iv. Surat Arahan KSN (Ketua Setiausaha Negara) :**

a) Surat Arahan KSN - 2006 Langkah-langkah Untuk Mengukuhkan Keselamatan *Wireless* LAN di Agensi-agensi Kerajaan;

b) Surat Arahan KSN – 2007 Langkah-langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit atau Lain-lain Peralatan Komunikasi;

**v. Surat Pekeliling Am**

a) Surat Pekeliling Perbendaharaan 5 Tahun 2007 – Tatacara Pengurusan Perolehan Kerajaan Secara Tender;

b) Surat Pekeliling Perbendaharaan Bilangan 5 Tahun 2009 – Perubahan Had Nilai dan Tatacara Pengurusan Perolehan Secara Sebut Harga;

c) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

d) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;

e) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

f) Surat Pekeliling Am Bilangan 3 2015 - Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat & Komunikasi (ICT) Agensi Sektor Awam;

g) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama)- “Tatacara Penyediaan, Penilaian dan PenerimaanTender”; dan

h) Surat Pekeliling Perbendaharaan Bil.3/1995 - “Peraturan Perolehan Perkhidmatan Perundingan”; dan

i) Surat Pekeliling Am Bilangan 4 Tahun 2024 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam.

**vi. Garis Panduan**

a) Garis Panduan Penggunaan ICT Ke Arah ICT Hijau dalam Perkhidmatan Awam: 3 Ogos 2010;
b) Garis Panduan Pelaksanaan Blog Bagi Agensi Sektor Awam: 17 Julai 2009;
c) Garis Panduan IT Outsourcing Agensi-agensi Sektor Awam: 2006;
d) *The Malaysian Government Interoperability Framework for Open Source Software (MYGIFOSS):* 2006;
e) Garis Panduan Penggunaan Biometrik Bagi Agensi-Agensi Sektor Awam 2004;
f) Garis Panduan Pengurusan Keselamatan ICT Sektor Awam Malaysia (MyMIS) yang dikeluarkan oleh MAMPU;
g) Garis Panduan Perolehan Hijau Kerajaan;
h) Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA); dan
i) Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2013 Dalam Sektor Awam;

**vii. Akta, Pekeliling, Arahan, Arahan Perbendaharaan, Garis Panduan, Perintah- Perintah Am dan Surat Pekeliling yang dikeluarkan oleh Kerajaan dari semasa ke semasa;**

**viii. Dasar – dasar kerajaan yang berkaitan; dan**

**ix. Dasar – dasar, Pekeliling, Surat Pekeliling dan Surat Edaran yang dikeluarkan oleh UMPSA dari semasa ke semasa**

**x. Polisi, Manual, Garis Panduan, Prosedur dan Standard Operating Prosedur (SOP) ICT UMPSA yang berkaitan dan sedang berkuatkuasa**

**LAMPIRAN 2**


## SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER UNIVERSITI MALAYSIA PAHANG AL-SULTAN ABDULLAH

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Agensi/Jabatan/Bahagian/Syarikat : .....

Saya dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan bersetuju untuk mematuhi Polisi Keselamatan Siber Universiti Malaysia Pahang Al-Sultan Abdullah; dan

2. Saya faham jika saya ingkar kepada mana-mana peruntukan di bawah Polisi Keselamatan Siber Universiti Malaysia Pahang Al-Sultan Abdullah, maka tindakan sewajarnya boleh diambil ke atas diri saya oleh Universiti Malaysia Pahang Al-Sultan Abdullah.

Saya dengan ini mengakui bahawa semua maklumat yang diberikan di atas adalah betul dan benar setakat pengetahuan dan kepercayaan saya. Saya faham bahawa sekiranya maklumat yang diberikan di atas adalah salah atau tidak benar pada apa-apa peringkat, saya boleh dikenakan tindakan di bawah undang-undang serta peraturan yang sedang berkuatkuasa.

Tandatangan : .....

Tarikh : .....

**Pengesahan Pegawai Keselamatan ICT**

.....

(Nama Pegawai Keselamatan ICT)

Tarikh: