UNIVERSITI SAINS ISLAM MALAYSIA
جَامِعَة العُلوم الإسْلامِيَة المَالِيزِية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

POLISI KESELAMATAN SIBER USIM V2.0



UNIVERSITI SAINS ISLAM MALAYSIA

ISI KANDUNGAN

1 PENGENALAN 1

1.1 LATAR BELAKANG 1

1.2 TUJUAN 1

1.3 OBJEKTIF 1

1.4 SKOP 2

1.5 PERNYATAAN POLISI KESELAMATAN SIBER 5

1.6 PRINSIP KESELAMATAN DATA DAN MAKLUMAT 5

1.6.1 Capaian Atas Dasar Perlu Mengetahui 5

1.6.2 Hak Capaian Minimum 6

1.6.3 Akauntabiliti 6

1.6.4 Pengasingan Tugas 6

1.6.5 Prinsip Kepercayaan Sifar (Zero Trust) 7

1.6.6 Pengauditan 7

1.6.7 Pematuhan 8

1.6.8 Pemulihan 8

1.6.9 Saling Bergantungan 8

1.6.10 Kawalan Capaian Berdasarkan Peranan 9

1.6.11 Prinsip Data Minimum 9

1.7 CIRI KESELAMATAN DATA DAN MAKLUMAT 9

1.7.1 Kerahsiaan 10

1.7.2 Integriti 10

1.7.3 Tidak Boleh Disangkal 10

1.7.4 Kesahihan 10

1.7.5 Ketersediaan 10

1.8 IMPLIKASI KETIDAKPATUHAN POLISI KESELAMATAN SIBER 11

2 TADBIR URUS 13

3 PENGURUSAN RISIKO 16

4 PELAN PENGURUSAN KESELAMATAN MAKLUMAT 20

5 KAWALAN ORGANISASI 23

5.1 POLISI KESELAMATAN SIBER 24

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT 27

5.3 PENGASINGAN TUGAS 44
5.4 TANGGUNGJAWAB PENGURUSAN 46
5.5 HUBUNGAN DENGAN PIHAK BERKUASA 47
5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS 48
5.7 PERISIKAN ANCAMAN 50
5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK 52
5.9 INVENTORI MAKLUMAT DAN ASET LAIN YANG BERKAITAN 55
5.10 PENGGUNAAN MAKLUMAT YANG BOLEH DITERIMA DAN ASET LAIN YANG BERKAITAN 57
5.11 PEMULANGAN ASET 60
5.12 PENGELASAN MAKLUMAT 61
5.13 PELABELAN MAKLUMAT 65
5.14 PEMINDAHAN DATA DAN MAKLUMAT 68
5.15 KAWALAN CAPAIAN 72
5.16 PENGURUSAN IDENTITI 77
5.17 MAKLUMAT PENGESAHAN IDENTITI 80
5.18 HAK CAPAIAN (*Access Rights*) 86
5.19 KESELAMATAN MAKLUMAT DALAM HUBUNGAN DENGAN PEMBEKAL 91
5.20 MENANGANI KESELAMATAN DALAM PERJANJIAN DENGAN PEMBEKAL 94
5.21 MENGURUS KESELAMATAN MAKLUMAT DALAM RANGKAIAN BEKALAN ICT 97
5.22 MEMANTAU, MENYEMAK DAN MENGURUS PERUBAHAN PERKHIDMATAN PEMBEKAL 98
5.23 KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN PENGKOMPUTERAN AWAN 100
5.24 PERANCANGAN DAN PENYEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT 102
5.25 PENILAIAN DAN KEPUTUSAN MENGENAI KEJADIAN KESELAMATAN MAKLUMAT 103
5.26 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT 104
5.27 PENGAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT 106
5.28 PENGUMPULAN BAHAN BUKTI 108
5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN 109
5.30 KESEDIAAN ICT BAGI KESINAMBUNGAN PERKHIDMATAN 112
5.31 KEPERLUAN PERUNDANGAN DAN KONTRAK 118
5.32 HAK HARTA INTELEK 120
5.33 PERLINDUNGAN REKOD 121

5.34 PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI 121
5.35 KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI 122
5.36 PEMATUHAN DASAR, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT 123
5.37 DOKUMENTASI PROSEDUR OPERASI STANDARD 124

6 KAWALAN SUMBER MANUSIA 126

6.1 TAPISAN KESELAMATAN 126
6.2 TERMA DAN SYARAT PERKHIDMATAN 128
6.3 KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT 129
6.4 PROSES TATATERTIB 129
6.5 TANGGUNGJAWAB SELEPAS PENAMATAN PERANAN ATAU JAWATAN 130
6.6 PERJANJIAN KERAHSIAAN ATAU KETAKDEDAHAN 133
6.7 BEKERJA SECARA JARAK JAUH 134
6.8 PELAPORAN INSIDEN KESELAMATAN MAKLUMAT 135

7 KAWALAN FIZIKAL 137

7.1 PERIMETER KESELAMATAN FIZIKAL 137
7.2 KEMASUKAN FIZIKAL 140
7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN 141
7.4 PEMANTAUAN KESELAMATAN FIZIKAL 142
7.5 PERLINDUNGAN DARIPADA ANCAMAN FIZIKAL DAN PERSEKITARAN 145
7.6 BEKERJA DI KAWASAN SELAMAT 145
7.7 POLISI MEJA KOSONG DAN SKRIN KOSONG 148
7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT 150
7.9 KESELAMATAN ASET DI LUAR PREMIS 155
7.10 MEDIA STORAN 156
7.11 UTILITI SOKONGAN 160
7.12 KESELAMATAN KABEL 161
7.13 PENYELENGGARAAN PERALATAN 163
7.14 PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN 164

8 KAWALAN TEKNOLOGI 168

8.1 PERIMETER KESELAMATAN FIZIKAL (PHYSICAL SECURITY PARAMETER) 168
8.2 HAK CAPAIAN ISTIMEWA 171
8.3 SEKATAN CAPAIAN MAKLUMAT 171

8.4 KAWALAN CAPAIAN KEPADA KOD SUMBER 173
8.5 PENGESAHAN IDENTITI YANG SELAMAT 175
8.6 PENGURUSAN KAPASITI 176
8.7 PERLINDUNGAN DARIPADA PERISIAN HASAD 177
8.8 PENGURUSAN KERENTANAN TEKNIKAL 180
8.9 PENGURUSAN KONFIGURASI 182
8.10 PENGHAPUSAN MAKLUMAT 183
8.11 PENYEMBUNYIAN DATA 184
8.12 PENCEGAHAN KETIRISAN DATA 185
8.13 SANDARAN MAKLUMAT 186
8.14 LEWAHAN BAGI KEMUDAHAN PEMPROSESAN MAKLUMAT 188
8.15 PENGELOGAN MAKLUMAT 190
8.16 AKTIVITI PEMANTAUAN 194
8.17 PENYEGERAKAN JAM 196
8.18 PENGGUNAAN PROGRAM UTILITI YANG MEMPUNYAI HAK ISTIMEWA 197
8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI 198
8.20 KESELAMATAN RANGKAIAN 200
8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN 204
8.22 PENGASINGAN RANGKAIAN 205
8.23 PENAPISAN WEB 205
8.24 PENGGUNAAN KRIPTOGRAFI 207
8.25 KITAR HAYAT PEMBANGUNAN SISTEM YANG SELAMAT 208
8.26 KEPERLUAN KESELAMATAN APLIKASI 210
8.27 PRINSIP REKA BENTUK DAN KEJURUTERAAN SISTEM YANG SELAMAT 214
8.28 PENGATURCARAAN PROGRAM SELAMAT 216
8.29 PENGUJIAN DAN PENERIMAAN KESELAMATAN SISTEM 217
8.30 PEMBANGUNAN SISTEM OLEH SUMBER LUAR 219
8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PRODUKSI 220
8.32 PENGURUSAN PERUBAHAN 224
8.33 DATA PENGUJIAN 229
8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PELAKSANAAN AUDIT 231

LAMPIRAN A 233

LAMPIRAN B 234

TAKRIFAN

(a)	*Antivirus*	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
(b)	Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
(c)	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.
(d)	*Backup* (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat.
(e)	Baki risiko	Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan.
(f)	*Bandwidth*	Jalur lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
(g)	PKP	Pelan Kesinambungan Perkhidmatan
(h)	CCTV	*Closed-Circuit Television System* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.

(i)	CIA	*Confidentiality, Integrity, Availability*
(j)	CDO	*Chief Digital Officer* Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan maklumat bagi menyokong arah tuju sesebuah organisasi.
(k)	*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.
(l)	*Data-at-rest* (data dalam simpanan)	*Refers to data that is being stored in stable destination systems. Data at rest is frequently defined as data that is not in use or is not traveling to system endpoints, such as mobile devices or workstations.*
(m)	*Data-in-motion* (data dalam pergerakan)	*Refers to a stream of data moving through any kind of network. It represents data which is being transferred or moved.*
(n)	*Data-in-use* (data dalam penggunaan)	*Refers to data that is not simply being passively stored in a stable destination, such as a central data warehouse, but is working its way through other parts of an IT architecture.*
(o)	*Denial of service*	Halangan pemberian perkhidmatan.
(p)	*Defence-in-depth*	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.

(q)	*Downloading*	Aktiviti muat turun sesuatu perisian.
(r)	*Encryption*	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
(s)	*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
(t)	*Forgery*	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft/espionage), penipuan (hoaxes).
(u)	CSIRT USIM	*Cyber Security Incident Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT USIM.
(v)	*Hard disk*	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
(w)	*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.
(x)	ICT	*Information and Communication Technology* Teknologi Maklumat dan Komunikasi

(y)	ICTSO	*Information and Communication Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
(z)	Impak teknikal	Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.
(aa)	Impak fungsi Universiti	Melibatkan perkara-perkara dari segi kewangan, reputasi, ketidakpatuhan dan pelanggaran privasi.
(bb)	Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
(cc)	Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
(dd)	*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.
(ee)	Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau Universiti dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
(ff)	ISDN	*Integrated Services Digital Network* Menggunakan isyarat digital pada talian telefon analog yang sedia ada.

(gg)	*Intrusion Detection System (IDS)*	Sistem Pengesan Pencerobohan 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.
(hh)	*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.
(ii)	ISMS	*Information Security Management System* Sistem Pengurusan Keselamatan Maklumat
(jj)	MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
(kk)	Keadaan Berisiko Tinggi	Dalam situasi yang mudah mendapat ancaman dari pihak luar atau apa-apa kemungkinan yang boleh menjejaskan kelancaran sistem.
(ll)	Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan

(mm)	Kriptografi	Kaedah untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
(nn)	LAN	Local Area Network Rangkaian Kawasan Setempat yang menghubungkan komputer.
(oo)	*Lock*	Mengunci komputer.
(pp)	*Logout*	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
(qq)	*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.
(rr)	*MFA*	Pengesahan Pelbagai Faktor (Multi-Factor Authentication) adalah proses pengesahan identiti digital yang menggunakan sekurang-kurangnya dua lapisan keselamatan berbeza (pengetahuan, pemilikan, atau biometrik) untuk mengurangkan risiko akses tanpa kebenaran akibat kebocoran kata laluan.
(ss)	*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, ActiveX dan sebagainya pada pelayar internet.

		MOdulator DEModulator
(tt)	MODEM	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.
(uu)	*Outsource*	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
(vv)	Pasukan ERT	Pasukan Tindakan Kecemasan/*Emergency Response Team* (ERT)
(ww)	Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
(xx)	Pengguna	Warga USIM, pembekal dan pihak-pihak lain yang diberi kebenaran menggunakan perkhidmatan ICT USIM.
(yy)	Pengolahan risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksana berdasarkan hasil penilaian risiko.
(zz)	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 Universiti

(aaa)	*Public-Key Infrastructure* (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
(bbb)	*Rollback* (undur)	Pengembalian pangkalan data atau program kepada keadaan stabil sebelum sesuatu ralat berlaku.
(ccc)	*Router*	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
(ddd)	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.
(eee)	*Screen saver*	Imej yang akan diaktifkan pada sistem/komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
(fff)	*Server*	Pelayan komputer
(ggg)	*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.

(hhh)	*Switches*	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense *Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu sistem penghantaran dengan mengurangkan perlanggaran yang berlaku.
(iii)	*Threat*	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
(jjj)	*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.
(kkk)	*Video Conference*	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna pada masa yang sama ia diterima oleh penghantar.
(lll)	*Video Streaming*	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
(mmr	Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
(nnn)	WAN	*Wide Area Network* Rangkaian yang merangkumi kawasan yang luas.

(ooo)	Warga USIM	Pelajar dan kakitangan yang berkhidmat di USIM sama ada berjawatan tetap, sambilan dan kontrak yang menggunakan perkhidmatan ICT USIM
(ppp)	Hak Capaian Logik (*Logical Access Rights*)	Kebenaran atau keistimewaan yang diberikan kepada pengguna untuk mengakses maklumat, sistem aplikasi, pangkalan data, rangkaian atau aset ICT berdasarkan peranan dan keperluan tugas.
(qqq)	SDEC	Pusat Pembangunan Sistem dan Kejuruteraan.
(rrr)	IOC	*Intelligent Operation Center*

REKOD PINDAAN DOKUMEN

Versi	Tarikh Perubahan	Deskripsi
1.0	22 April 2022	Versi pertama dokumen
1.1	28 Februari 2024	Kemas kini kecil
2.0	29 Oktober 2026	Perubahan besar / semakan penuh

1 PENGENALAN

1.1 LATAR BELAKANG

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

1.2 TUJUAN

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

1.3 OBJEKTIF

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

(a) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dalam aspek kerahsiaan, integriti, kebolehsediaan, dan kesahihan maklumat serta penyangkalan;

(b) Mematuhi keperluan perundangan, peraturan, standard, pekeliling dan prosedur yang sedang berkuat kuasa;

(c) Melaksanakan pengurusan risiko dan insiden keselamatan siber yang lebih berkesan (Pengurusan risiko di bawah tanggungjawab I-ROSH);

(d) Memastikan penyampaian perkhidmatan USIM pada tahap keselamatan tertinggi yang dapat meningkatkan keyakinan pihak berkepentingan seperti Universiti kerajaan, industri, dan orang awam;

(e) Menjamin kelancaran operasi dan kesinambungan perkhidmatan USIM dengan meminimumkan impak insiden keselamatan maklumat fizikal dan logikal;

(f) Memudahkan perkongsian maklumat yang selamat dan terjamin;

(g) Mencegah sebarang penyalahgunaan atau kecurian maklumat kerajaan; dan

(h) Menyediakan asas bagi penambahbaikan yang berterusan dalam pengurusan keselamatan dan pentadbiran teknologi maklumat dan komunikasi.

1.4 SKOP

PKS USIM merupakan panduan utama bagi semua warga USIM serta pihak-pihak yang terlibat dalam pengurusan data atau maklumat di Universiti ini. Polisi ini memperincikan peranan, tanggungjawab, arahan, peraturan, garis panduan, dan amalan yang **WAJIB DIBACA, DIFAHAMI, dan DIPATUHI** oleh semua warga Universiti, termasuk pembekal, pakar runding, serta pihak-pihak yang terlibat dengan perkhidmatan teknologi maklumat dan komunikasi USIM.

Polisi ini juga terpakai untuk pelindungan terhadap kesemua aset maklumat Universiti Sains Islam Malaysia, yang meliputi data dan maklumat dalam bentuk digital (*softcopy*) atau bercetak (*hardcopy*), perkakasan, perisian, infrastruktur ICT,

manusia, dan premis. Aset-aset ini adalah sangat penting dan sangat berharga, memastikan Universiti Sains Islam Malaysia dapat menjalankan urusan rasmi Kerajaan dengan lancar kepada masyarakat, sektor swasta, serta Universiti yang berkaitan.

PKS USIM menetapkan keperluan asas seperti yang berikut:

(a) **Kebolehcapaian Data dan Maklumat:** Data dan maklumat mesti dapat dicapai secara berterusan dengan pantas, tepat, mudah, dan boleh dipercayai. Ini adalah penting untuk memastikan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.

(b) **Kerahsiaan dan Kesempurnaan Maklumat:** Semua data dan maklumat hendaklah dilindungi kerahsiaannya dan dikendalikan dengan baik pada setiap masa untuk memastikan ketepatan serta melindungi kepentingan kerajaan, perkhidmatan, dan masyarakat.

Untuk memastikan keselamatan aset maklumat sepanjang masa, PKS USIM meliputi perlindungan semua bentuk maklumat kerajaan yang diwujudkan, diproses, disimpan, dihantar, sedang digunakan, diedarkan, disimpan, diselenggara, dihapuskan dan dimusnahkan serta diarkibkan dalam persekitaran ICT USIM. Perlindungan ini dilaksanakan melalui sistem kawalan dan prosedur pengendalian yang menyeluruh bagi elemen-elemen yang berikut:

(a) **Data atau Maklumat**: Koleksi fakta dalam bentuk kertas atau mesej elektronik yang digunakan untuk mencapai misi dan objektif Universiti. Contohnya, sistem dokumentasi, prosedur operasi, rekod, pangkalan data, dan arkib maklumat.

(b) **Salinan Digital (*Softcopy*):** Fakta dalam bentuk digital yang digunakan

untuk mencapai misi dan objektif Universiti, termasuk rekod digital, pangkalan data, dan maklumat arkib.

(c) **Salinan Bercetak (*Hardcopy*):** Fakta dalam bentuk bercetak, seperti sistem dokumentasi, prosedur operasi, rekod, dan fail-fail.

(d) **Perkakasan (*Hardware*):** Semua aset fizikal yang menyokong pemprosesan dan penyimpanan maklumat, termasuk komputer, pelayan, dan peralatan komunikasi.

(e) **Perisian (*Software*):** Program dan dokumentasi yang berkaitan dengan sistem komputer, termasuk perisian aplikasi dan sistem operasi yang digunakan untuk pemprosesan maklumat di Universiti.

(f) **Infrastruktur ICT**: Set lengkap perkakasan, perisian, rangkaian, dan kemudahan yang menyokong pemprosesan, penyimpanan, dan penghantaran maklumat dalam organisasi. Ini termasuk LAN, WAN, sistem kad akses, perkhidmatan pengkomputeran awan, serta kemudahan sokongan seperti bekalan elektrik dan sistem pencegah kebakaran.

(g) **Manusia**: Individu yang memiliki pengetahuan dan kemahiran untuk melaksanakan tugas harian bagi mencapai misi dan objektif Universiti. Mereka ialah aset berdasarkan tugas dan peranan yang mereka laksanakan.

(h) **Premis**: Semua kemudahan dan premis yang menempatkan aset-aset di atas, yang mesti dilindungi dengan ketat untuk mencegah kebocoran rahsia atau kelemahan perlindungan, yang akan dianggap sebagai pelanggaran keselamatan.

Polisi ini memastikan bahawa setiap aspek di atas diberikan perlindungan yang sewajarnya, meminimumkan risiko dan mengekalkan integriti operasi USIM.

1.5 PERNYATAAN POLISI KESELAMATAN SIBER

USIM komited untuk mengekalkan persekitaran yang selamat bagi aset maklumat dengan melaksanakan kawalan keselamatan siber yang berkesan selaras dengan standard dan rangka kerja keselamatan siber yang ditetapkan oleh Universiti ini.

1.6 PRINSIP KESELAMATAN DATA DAN MAKLUMAT

Prinsip keselamatan hendaklah dipilih berdasarkan penilaian risiko dan kategori maklumat yang dikendalikan oleh sistem. Bagi mencapai objektif keselamatan maklumat, USIM hendaklah melaksanakan prinsip keselamatan seperti yang berikut:

1.6.1 Capaian Atas Dasar Perlu Mengetahui

USIM 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.

1.6.2 Hak Capaian 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.

1.6.3 Akauntabiliti

Semua pengguna bertanggungjawab ke atas semua tindakannya terhadap aset maklumat USIM. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap perlindungan keselamatan yang diperlukan oleh sesuatu sumber/aset maklumat. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesahkan bahawa pengguna sistem ICT tersebut boleh dipertanggungjawabkan atas tindakan mereka.

1.6.4 Pengasingan Tugas

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

1.6.5 Prinsip Kepercayaan Sifar (Zero Trust)

Prinsip ini menegaskan bahawa tiada pengguna, peranti, atau rangkaian harus dipercayai secara automatik, sama ada berada dalam atau luar perimeter rangkaian. Setiap permintaan untuk mencapai data atau maklumat mesti melalui proses pengesahan yang teliti sebelum hak capaian diberikan. Prinsip ini menyatakan bahawa:

(a) semua trafik rangkaian (dalaman dan luaran) dianggap sebagai tidak dipercayai;

(b) Capaian kepada sumber diberikan berdasarkan set kriteria yang komprehensif dan dinamik, termasuk identiti pengguna, keadaan dan kesihatan peranti, lokasi capaian, serta faktor konteks lain yang relevan. Capaian kepada sumber hanya akan diluluskan selepas pengesahan menyeluruh terhadap identiti pengguna dan status peranti, tanpa mengira lokasi fizikal, untuk memastikan keselamatan yang maksimum; dan

(c) menekankan prinsip keistimewaan yang paling sedikit, capaian kepada sumber yang perlu dicapai akan diberikan berdasarkan keperluan, apabila diperlukan dan hanya untuk tempoh masa yang ditetapkan.

1.6.6 Pengauditan

Pengauditan ialah tindakan untuk menilai, memeriksa, serta menganalisis aktiviti, rekod dan proses yang telah dilaksanakan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Tujuannya

adalah untuk memastikan bahawa aktiviti tersebut mematuhi peraturan, piawaian, dan prosedur yang ditetapkan serta untuk mengidentifikasi sebarang isu, ketidakpatuhan, atau potensi risiko. Oleh itu, aset maklumat seperti komputer, pelayan, penghala rangkaian (network router), tembok keselamatan (firewall) dan peralatan rangkaian **hendaklah dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit**.

1.6.7 Pematuhan

Polisi Keselamatan Siber Universiti Sains Islam Malaysia hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan maklumat.

1.6.8 Pemulihan

Pemulihan sistem amat perlu untuk memastikan kesediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan.

1.6.9 Saling Bergantungan

Setiap prinsip keselamatan adalah saling melengkapi dan bergantung antara satu dengan lain untuk membentuk sistem keselamatan yang menyeluruh dan berkesan. Prinsip-prinsip ini tidak boleh dilaksanakan secara terpisah, tetapi mesti diintegrasikan dan diselaraskan untuk mencapai keselamatan yang maksimum.

1.6.10 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.

1.6.11 Prinsip Data Minimum

USIM hendaklah mengamalkan prinsip peminimuman data yang mengehadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

1.7 CIRI KESELAMATAN DATA DAN MAKLUMAT

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:

1.7.1 Kerahsiaan

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

1.7.2 Integriti

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

1.7.3 Tidak Boleh Disangkal

Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal.

1.7.4 Kesahihan

Data dan maklumat hendaklah sah serta disahkan daripada punca yang dipercayai.

1.7.5 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 USIM, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah-langkah pencegahan yang perlu diambil untuk menangani risiko berkenaan.

1.8 IMPLIKASI KETIDAKPATUHAN POLISI KESELAMATAN SIBER

Ketidakpatuhan terhadap Polisi Keselamatan Siber USIM boleh mengakibatkan pelbagai implikasi yang serius, termasuk tetapi tidak terhad kepada:

(a) **Risiko Keselamatan:** Ketidakpatuhan boleh menyebabkan pendedahan data sensitif, pencerobohan sistem, atau gangguan operasi, yang boleh mengakibatkan kehilangan maklumat penting atau kerosakan kepada infrastruktur digital.

(b) **Gangguan Operasi:** Ketidakpatuhan boleh menyebabkan gangguan kepada operasi harian Universiti, termasuk masa henti sistem, kehilangan data, dan kerosakan peralatan, yang boleh memberi kesan langsung kepada penyampaian perkhidmatan.

(c) **Kesan Undang-Undang**: Kegagalan mematuhi polisi ini boleh menyebabkan tindakan undang-undang diambil terhadap pihak yang terlibat, termasuk denda atau tindakan undang-undang lain yang berkaitan dengan pelanggaran peraturan dan undang-undang keselamatan siber.

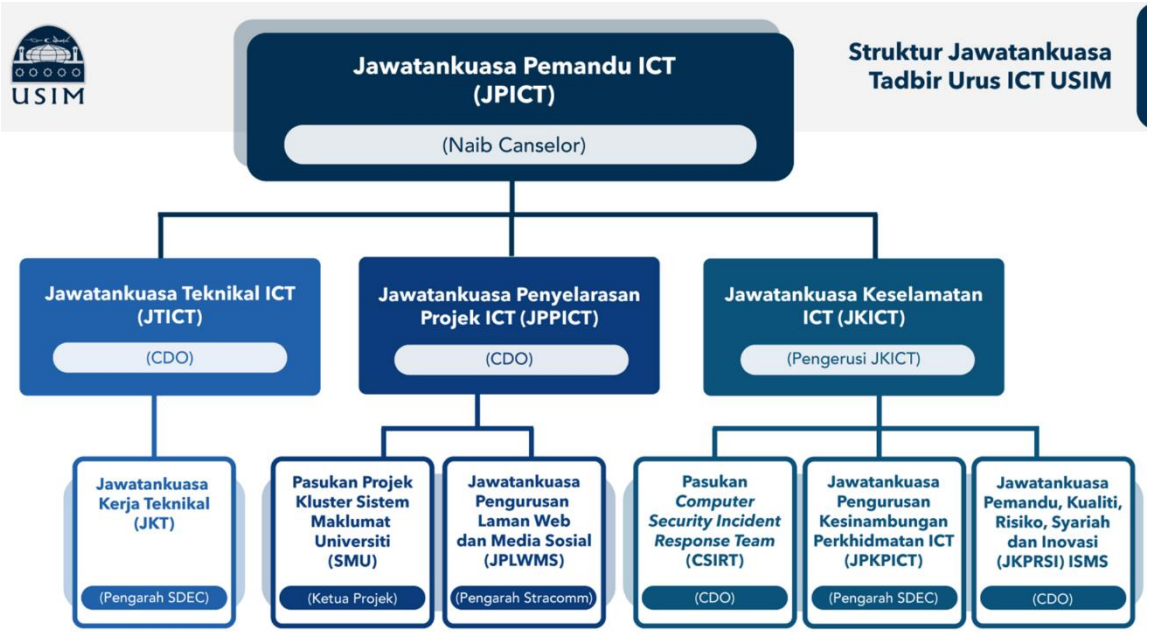
(d) **Kerugian Kewangan:** Ketidakpatuhan boleh membawa kepada kerugian kewangan yang besar, sama ada melalui denda, kos pemulihan, atau kehilangan kepercayaan pelanggan dan pihak berkepentingan yang boleh menjejaskan kedudukan kewangan Universiti.

(e) **Kerosakan Reputasi:** Insiden keselamatan siber yang disebabkan oleh ketidakpatuhan boleh merosakkan reputasi USIM, mengurangkan kepercayaan pihak berkepentingan dan masyarakat umum terhadap keupayaan USIM dalam menguruskan keselamatan maklumat.

(f) **Tindakan Disiplin:** Warga USIM yang didapati tidak mematuhi PKS ini boleh dikenakan tindakan disiplin, termasuk amaran, penggantungan, atau penamatan perkhidmatan, bergantung kepada tahap pelanggaran yang dilakukan.

2 TADBIR URUS

Bagi memastikan keberkesanan dan kejayaan pelaksanaan Polisi Keselamatan Siber (PKS) USIM, struktur tadbir urus ICT universiti diwujudkan di bawah Jawatankuasa Pemandu ICT Universiti (JPICT) yang dipengerusikan oleh Naib Canselor sebagai platform utama penetapan dasar, penyelarasan dan pemantauan tadbir urus ICT universiti:



Rajah 1: Struktur Jawatankuasa Tadbir Urus ICT USIM

Di bawah JPICT, terdapat tiga jawatankuasa utama yang memainkan peranan khusus dalam pelaksanaan dan pemantauan inisiatif ICT universiti, iaitu:

(a) **Jawatankuasa Teknikal ICT (JTICT) –** dipengerusikan oleh CDO, bertanggungjawab terhadap aspek teknikal ICT melalui Jawatankuasa Kerja Teknikal (JKT) di bawah seliaan Pengarah SDEC.

(b) **Jawatankuasa Penyelaras Projek ICT (JPPICT) –** diketuai oleh CDO, menyelaras pelaksanaan projek ICT universiti termasuk Pasukan Projek

Kluster Sistem Integrasi Aplikasi Universiti (SINAR) dan Jawatankuasa Pengurusan Laman Web dan Media Sosial (JPLWMS) di bawah Pengarah Stracomm.

(c) **Jawatankuasa Keselamatan ICT (JKICT)** – dipengerusikan oleh Pengerusi JKICT, dan keahlian terdiri daripada pakar rujuk bidang serta Pegawai Keselamatan ICT (Information and Communication Security Officer, ICTSO) yang memantau hal ehwal keselamatan maklumat melalui beberapa sub-jawatankuasa khusus seperti:

(i) Pasukan *Cyber Security Incident Response Team* (CSIRT USIM)

(ii) Jawatankuasa Pengurusan Kesinambungan Perkhidmatan ICT (JPKPICT)

(iii) Jawatankuasa Pemandu, Kualiti, Risiko, Syariah dan Inovasi ISMS (JKPRSI ISMS)

Struktur ini memastikan tadbir urus keselamatan maklumat dan kesinambungan perkhidmatan ICT di USIM dilaksanakan secara menyeluruh berpaksikan kepada dasar serta piawaian universiti.

Bidang rujukan Jawatankuasa Pemandu ICT USIM (JPICT USIM) adalah seperti berikut:

(a) Menetapkan arah tuju dan strategi untuk pelaksanaan pendigitalan Universiti;

(b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan hala tuju/strategi ICT agensi;

(c) Meluluskan projek pendigitalan Universiti berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan;

(d) Menyelaras dan menyeragamkan pelaksanaan pendigitalan agar selari dengan Pelan Strategik ICT Universiti (ISP) / Pelan Strategik Pendigitalan (PSP);

(e) Mengikuti dan memantau perkembangan program pendigitalan Universiti serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan program pendigitalan;

(f) Membantu Naib Canselor dalam membuat keputusan-keputusan penting berkenaan inisiatif pendigitalan di peringkat Universiti;

(g) Platform bagi ahli mesyuarat untuk membentangkan kertas kerja berkaitan pendigitalan bagi mendapatkan nasihat dan kelulusan ahli mesyuarat;

(h) Platform bagi ahli mesyuarat untuk memaklumkan garis panduan, polisi, prosedur pendigitalan / ICT untuk mendapatkan kelulusan ahli-ahli mesyuarat;

(i) Mengesahkan laporan semasa inisiatif pendigitalan Universiti;

(j) Meluluskan di peringkat Universiti bagi projek pendigitalan / ICT bagi mendapatkan perakuan / kelulusan selanjutnya daripada Jawatankuasa Teknikal ICT Kementerian Pendidikan Tinggi (JTI KPT) / Jawatankuasa Pemandu ICT Kementerian Pendidikan Tinggi (JPICT KPT) / Jawatankuasa Teknikal ICT Sektor Awam Jabatan Digital Negara (JTISA) dan

(k) Hal-hal lain berkaitan pendigitalan yang difikirkan perlu.

3 PENGURUSAN RISIKO

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

Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya **dua kali** setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber USIM.

Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya **dua kali setahun** dan dimaklumkan kepada Jawatankuasa Pemandu, Kualiti, Risiko, Syariah dan Inovasi ISMS (JKPRSI ISMS).

Penilaian risiko keselamatan maklumat harus dilaksanakan ke atas semua aset maklumat USIM, termasuk aset fizikal, aplikasi, perisian, pelayan, rangkaian, serta proses dan prosedur yang berkaitan. Selain itu, penilaian risiko ini juga perlu dijalankan di premis yang menempatkan aset maklumat seperti pusat data, bilik media storan, kemudahan utiliti, dan sistem-sistem sokongan lain.

Pelaksanaan pengurusan risiko hendaklah selaras dengan Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024. Dalam menghadapi potensi risiko, semua pihak yang terlibat perlu mengenal pasti tindakan yang sewajarnya, termasuk:

(a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

(b) Menerima atau bersedia menghadapi risiko yang mungkin berlaku selagi risiko tersebut tidak menjejaskan penyampaian perkhidmatan USIM;

(c) Mengelakkan atau mencegah risiko dengan mengambil langkah-langkah yang dapat mengelakkan atau mencegah terjadinya risiko; dan

(d) Memindahkan risiko kepada pihak ketiga seperti pembekal, pakar runding, atau pihak berkepentingan lain.

Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

(a) Kerentanan

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

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

(c) Impak

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

(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

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

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

- Teknologi

  Teknologi hendaklah dikenal pasti untuk mengurangkan risiko. Sebagai contoh, tembok api digunakan untuk mengehadkan capaian logikal kepada sistem tertentu.

- Proses

  Perekayasaan proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

- Manusia

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

(f) Pengurusan Risiko

Penyedia perkhidmatan digital di USIM 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.

4 PELAN PENGURUSAN KESELAMATAN MAKLUMAT

Setiap projek di USIM hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain.

Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), PKS USIM dan surat pekeliling/arahan yang sedang berkuat kuasa untuk menangani isu keselamatan operasi semasa projek dilaksanakan.

Pelan ini hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.

Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen yang berikut:

(a) Peranti Pengkomputeran Peribadi

(i) Peranti Pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, telefon pintar, tablet dan peranti storan.

(ii) Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada USIM. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

(b) Peranti Rangkaian

(i) Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti *switch*, penghala rangkaian, tembok keselamatan, peranti Virtual Private Network (VPN) dan kabel.

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

(c) Aplikasi

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

(ii) 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.

(d) Pelayan (*Server*)

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

(ii) 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.

(e) Persekitaran Fizikal

(i) Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan aset ICT.

(ii) USIM 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.

(iii) Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip kawalan defend-in-depth.

(iv) 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.

5 KAWALAN ORGANISASI

Terdapat 37 kawalan organisasi yang terpakai dan perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di USIM. Perincian kawalan organisasi seperti di bawah.

5.1 POLISI KESELAMATAN SIBER

ID	KETERANGAN	PERANAN
5.1.1	**Pelaksanaan Polisi** Pelaksanaan polisi ini akan dijalankan oleh Naib Canselor dengan disokong oleh Jawatankuasa Pemandu ICT (JPICT), Jawatankuasa Keselamatan ICT (JKICT), Jawatankuasa Pemandu ISMS & PKP yang terdiri daripada Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO), Pengarah SDEC dan ahli-ahli yang dilantik oleh Naib Canselor. Polisi Keselamatan Siber USIM mestilah dipatuhi oleh semua warga USIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT USIM. Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan USIM kepada warga USIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT USIM.	Naib Canselor, JPICT, JKICT, CDO, ICTSO, Pengarah SDEC
5.1.2	**Pengesahan Polisi** Polisi itu perlu diperakui di peringkat pengurusan tertinggi USIM.	Lembaga Pengurusan Universiti (LPU)

ID	KETERANGAN	PERANAN
5.1.3	**Penguatkuasaan Polisi** PKS USIM mestilah dipatuhi oleh semua warga Universiti, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di USIM. Sebarang ketidakpatuhan kepada dasar ini boleh mengakibatkan tindakan tatatertib termasuk sebarang remedi/tindakan undang-undang lain di bawah akta/peraturan/undang-undang semasa yang berkuat kuasa.	Warga USIM, Pihak yang terlibat dalam perkhidmatan ICT di USIM
5.1.4	**Penyebaran Polisi** Program kesedaran tentang PKS USIM ini hendaklah diatur dan diselaraskan.	ICTSO, Pengarah SDEC
5.1.5	**Pengecualian Polisi** Keselamatan ICT Universiti terpakai kepada warga USIM dan pembekal serta semua pihak yang terlibat dalam pembekalan perkhidmatan ICT dan tiada pengecualian diberikan.	Warga USIM, Pihak yang terlibat dalam perkhidmatan ICT di USIM

ID	KETERANGAN	PERANAN
5.1.6	**Kajian Semula/penyelenggaraan Polisi** Kajian semula dan penyelenggaraan dasar hendaklah dilaksanakan mengikut keperluan. Semua dokumen dan rekod hendaklah dilindungi dan dikawal mengikut undang-undang / arahan / peraturan / garis panduan semasa yang berkuat kuasa. (a) Mengenal pasti dan menentukan perubahan yang diperlukan; (b) Mengemukakan cadangan pindaan untuk tindakan dan pertimbangan kepada JPICT bagi tujuan pengesahan dan dibentangkan kepada Lembaga Pengarah Universiti (LPU) bagi tujuan pemakaian di USIM; (c) Memaklumkan pindaan yang telah disahkan oleh JPICT dan diluluskan oleh LPU kepada warga USIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT USIM; dan (d) Polisi ini hendaklah dikaji semula sekurang-kurangnya sekali dalam tempoh **TIGA (3) TAHUN SEKALI** atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	JPICT, CDO, JKICT, ICTSO

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.2.1	**Peranan dan Tanggungjawab Keselamatan Maklumat** Peranan dan tanggungjawab adalah seperti yang berikut: (a) **Naib Canselor** **Tanggungjawab:** (i) Memastikan penguatkuasaan pelaksanaan polisi ini; (ii) Memastikan warga USIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT USIM memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini; (iii) Memastikan semua keperluan USIM seperti sumber kewangan, personel dan	Naib Canselor, Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO), Pengarah SDEC, Pentadbir Sistem ICT Jawatankuasa Keselamatan ICT (JKICT), Jawatankuasa Pemandu ICT (JPICT), Jawatankuasa Pemandu ISMS, Cyber Security Incident Response Team (CSIRT) USIM, Pengguna

ID	KETERANGAN	PERANAN
	perlindungan keselamatan adalah mencukupi; (iv) Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam polisi ini; dan (v) Melantik CDO, ICTSO dan ahli jawatankuasa yang terlibat dalam pelaksanaan polisi ini.	

ID	KETERANGAN	PERANAN
	(b) **Ketua Pegawai Digital (CDO)** Peranan dan tanggungjawab CDO adalah seperti yang berikut: **Tanggungjawab:** (i) Membantu Naib Canselor dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan di dalam polisi ini; (ii) Memastikan kawalan keselamatan maklumat dalam USIM diseragam dan diselaraskan dengan sebaiknya; (iii) Memastikan dokumen strategik ICT seperti Pelan Strategik ICT USIM hendaklah mengandungi aspek keselamatan siber; dan (iv) Menyelaras pelan latihan dan program kesedaran keselamatan siber.	

ID	KETERANGAN	PERANAN
	(c) **Pegawai Keselamatan ICT (ICTSO)** Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti yang berikut: **Tanggungjawab:** (i) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan polisi ini; (ii) Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat yang berkuat kuasa; (iii) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlakunya ancaman keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (iv) Melaporkan insiden keselamatan siber kepada CSIRT USIM dan seterusnya membantu dalam penyiasatan atau pemulihan;	

ID	KETERANGAN	PERANAN
	(v) Melaporkan insiden keselamatan siber kepada CDO; (vi) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera; (vii) Memastikan pematuhan Polisi ini dalam kalangan warga USIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT USIM; (viii) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber; dan Menyedia dan merangka latihan dan program kesedaran keselamatan siber.	

ID	KETERANGAN	PERANAN
	(d) **Pengarah SDEC** Peranan dan tanggungjawab Pengarah SDEC ialah melaksanakan keperluan polisi ini dalam operasi semasa seperti yang berikut: **Tanggungjawab:** (i) Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; (ii) Pembelian atau peningkatan perisian dan sistem komputer; (iii) Perolehan teknologi dan perkhidmatan komunikasi baharu; (iv) Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan; dan (v) Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat kerajaan yang berkuat kuasa.	

ID	KETERANGAN	PERANAN
	(e) **Pentadbir Sistem ICT** Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti yang berikut: **Tanggungjawab:** (i) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai personel yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (ii) Menentukan ketepatan dan kesahihan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi ini; (iii) Memantau aktiviti capaian sistem aplikasi, rangkaian, pangkalan data, pengurusan server dan keselamatan siber;	

ID	KETERANGAN	PERANAN
	(iv) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta; (v) Menganalisis dan menyimpan rekod jejak audit; dan (vi) Menyediakan laporan mengenai aktiviti capaian secara berkala.	

ID	KETERANGAN	PERANAN
	(f) **Pemilik Sistem** Pemilik Sistem adalah Jabatan / Pusat / Bahagian / Unit yang memberikan sesuatu perkhidmatan sistem aplikasi dan mempunyai kepentingan secara langsung serta mendapat faedah daripada Pembangunan Sistem. **Tanggungjawab:** (i) Mengetuai Mesyuarat Sistem; (ii) Menyediakan kertas cadangan konsep pembangunan sistem aplikasi; (iii) Memastikan keperluan pembangunan sistem ditakrifkan dengan jelas (*system requirement*);	

ID	KETERANGAN	PERANAN
	(iv) Memastikan sumber manusia mencukupi bagi tujuan pembangunan sistem aplikasi dan tidak bertindih dengan pembangunan sistem aplikasi yang sedang berjalan; (v) Menempatkan individu yang berpengetahuan dan berpengalaman (*subject matter expert*) di dalam pasukan projek bagi membantu pembangunan sistem; (vi) Memastikan sebarang *Standard of Procedure* (SOP) disediakan, dikemas kini bagi tujuan pelaksanaan Sistem Aplikasi yang dibangunkan; dan (vii) Memastikan sistem diuji, diselenggara dan ditambah baik (jika perlu) secara berkala.	

ID	KETERANGAN	PERANAN
	(g) **Jawatankuasa Keselamatan ICT (JKICT)** Peranan dan tanggungjawab Jawatankuasa Keselamatan ICT (JKICT) adalah seperti yang berikut: **Tanggungjawab:** (i) Pelaksanaan promosi sistem	

ID	KETERANGAN	PERANAN
	kepada pengguna sasaran; (ii) Membangun, menilai dan mengkaji semula Dasar Keselamatan ICT USIM dari semasa ke semasa; (iii) Menyebar dan menguatkuasakan Dasar Keselamatan ICT kepada Warga USIM dan memantau pematuhannya; (iv) Menerima aduan insiden keselamatan ICT dan menjalankan siasatan teknikal ke atas sebarang pelanggaran Dasar; (v) Menyediakan laporan insiden keselamatan ICT berdasarkan laporan daripada CSIRT USIM dan mengemukakan kepada Jawatankuasa Tatatertib Kakitangan bagi kakitangan dan Pihak Berkuasa Tatatertib Pelajar bagi pelajar; dan (vi) Memantau dan menambahbaik kaedah pelaksanaan keselamatan ICT di USIM. (h) **Jawatankuasa Pemandu ICT (JPICT)** Peranan dan tanggungjawab JPICT seperti yang terkandung dalam **Surat Pekeliling Am Bil 3 Tahun 2015: Garis Panduan Permohonan Kelulusan Teknikal dan**	

ID	KETERANGAN	PERANAN
	Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Agensi Sektor Awam bagi pengurusan keselamatan siber. **Tanggungjawab:** (i) Menetap arah tuju dan strategik untuk pelaksanaan ICT universiti; (ii) Meluluskan projek ICT Universiti berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan; (iii) Menyelaras dan menyeragamkan pelaksanaan ICT agar selari dengan Pelan Strategik ICT Universiti; (iv) Mengikuti dan memantau perkembangan program ICT Universiti serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT; (v) Membantu Naib Canselor dalam membuat keputusan-keputusan penting berkenaan ICT di peringkat Universiti; (vi) Platform bagi ahli mesyuarat untuk membentangkan kertas kerja berkaitan ICT bagi mendapatkan	

ID	KETERANGAN	PERANAN
	nasihat dan kelulusan ahli mesyuarat; (vii) Platform bagi ahli mesyuarat untuk memaklumkan garis panduan, polisi, prosedur ICT untuk mendapatkan kelulusan ahli-ahli mesyuarat; (viii) Mengesahkan laporan semasa ICT Universiti; dan (ix) Meluluskan projek ICT untuk tahun hadapan bagi mendapatkan kelulusan daripada Jawatankuasa Pemandu Kementerian Pengajian Tinggi (JPICT KPT) dan Jawatankuasa Teknikal ICT Sektor Awam (JTISA). (i) **Jawatankuasa Pemandu, Kualiti, Risiko, Syariah dan Inovasi ISMS (JKPRSI ISMS)** Bidang rujukan adalah seperti berikut: **Tanggungjawab:** (i) Menentukan hala tuju keseluruhan pelaksanaan pensijilan ISMS USIM yang merangkumi perancangan, pemantauan dan pengesahan terhadap: (ii) Pelaksanaan pensijilan ISMS ke atas perkhidmatan USIM yang dikenal pasti;	

ID	KETERANGAN	PERANAN
	(iii) Kelulusan ke atas dasar, objektif dan skop pelaksanaan ISMS; (iv) Penetapan kriteria penerimaan risiko, tahap risiko dan risk treatment plan; (v) Kajian semula pelaksanaan pensijilan ISMS ke atas perkhidmatan-perkhidmatan USIM yang dikenal pasti; (vi) Dasar dan objektif ISMS diwujudkan selaras dengan hala tuju strategik USIM; (vii) Keperluan ISMS diterapkan dalam budaya kerja pegawai USIM; (viii) Sumber yang diperlukan oleh pasukan pelaksana ISMS; (ix) Kepentingan pengurusan ISMS yang berkesan dan pematuhan terhadap keperluannya; (x) Pencapaian sasaran ISMS seperti yang dirancang; (xi) Arahan dan sokongan kepada Pasukan ISMS USIM bagi memastikan ISMS dapat dilaksanakan dengan berkesan; dan (xii) Pelaksanaan program penambahbaikan dan peningkatan ISMS yang berterusan. **Meluluskan**:	

ID	KETERANGAN	PERANAN
	• Struktur organisasi ISMS dan PKP USIM; • Keperluan sumber; dan • Pelantikan Pasukan Audit dalam ISMS USIM. (j) **Cyber Security Incident Response Team (CSIRT USIM)** Peranan dan tanggungjawab CSIRT USIM adalah seperti yang berikut: **Tanggungjawab:** (i) Menerima dan mengesan aduan keselamatan siber serta menilai tahap dan jenis insiden; (ii) Merekod dan menjalankan siasatan awal insiden yang diterima; (iii) Menangani tindak balas insiden keselamatan siber dan mengambil tindakan baik pulih minimum; (iv) Menasihati Pentadbir Sistem ICT untuk mengambil tindakan pemulihan dan pengukuhan; dan (v) Menyebarkan makluman berkaitan pengukuhan keselamatan siber kepada Pentadbir Sistem ICT.	

	(k) **Pengguna Sistem atau Aset Maklumat** Peranan dan tanggungjawab pengguna adalah seperti yang berikut: **Tanggungjawab:** (i) Membaca, memahami dan mematuhi PKS USIM ini; (ii) Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakannya; (iii) Menjalani tapisan keselamatan sekiranya di perlukan di kehendaki berurusan dengan maklumat rasmi terperingkat; (iv) Mematuhi prinsip-prinsip keselamatan yang dinyatakan dalam PKS ini dan menjaga kerahsiaan maklumat Universiti/Kerajaan; (v) Melaksanakan langkah-langkah perlindungan seperti yang berikut: • Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; • Memeriksa maklumat dan menentukan maklumat tersebut sentiasa tepat dan lengkap dari semasa ke semasa; • Menentukan maklumat sedia untuk digunakan;	

	• Menjaga kerahsiaan maklumat; • Mematuhi dasar, piawaian dan garis panduan keselamatan siber yang ditetapkan; • Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan pemprosesan, penyimpanan penghantaran, penyampaian, pertukaran dan pemusnahan; dan • Menjaga kerahsiaan kawalan keselamatan siber dari diketahui umum. (vi) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CSIRT USIM dengan segera; (vii) Menghadiri program-program kesedaran mengenai keselamatan siber; dan (viii) Bersetuju dengan terma dan syarat yang terkandung dalam PKS USIM ini.	

5.3 PENGASINGAN TUGAS

ID	KETERANGAN	PERANAN
5.3.1	**Pengasingan Tugas** Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan risiko penyalahgunaan, peluang mengubah suai tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) 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;	Ketua PTJ

ID	KETERANGAN	PERANAN
	(b) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai produksi; (c) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; (d) Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya; dan (e) Semakan dan pemantauan hak capaian perkakasan, perisian dan sistem hendaklah dilaksanakan secara berkala.	

5.4 TANGGUNGJAWAB PENGURUSAN

ID	KETERANGAN	PERANAN
5.4.1	**Tanggungjawab Pengurusan** Pengurusan hendaklah memastikan warga USIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT USIM supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.	CDO, ICTSO, Ketua PTJ, Pentadbir Sistem ICT

5.5 HUBUNGAN DENGAN PIHAK BERKUASA

ID	KETERANGAN	PERANAN
5.5.1	**Hubungan dengan Pihak Berkuasa** Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab USIM; (b) Mewujud dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia dan Suruhanjaya Komunikasi Dan Multimedia. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan (c) Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.	I-ROSH

5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS

ID	KETERANGAN	PERANAN
5.6.1	**Hubungan dengan Kumpulan Berkepentingan yang Khusus** Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau forum yang berkaitan bagi: (a) Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat; (b) Memastikan pemahaman tentang persekitaran keselamatan maklumat adalah terkini; (c) Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini;	CDO

ID	KETERANGAN	PERANAN
	(d) Mendapat capaian kepada nasihat pakar keselamatan maklumat; (e) Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan (f) Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	

5.7 PERISIKAN ANCAMAN

ID	KETERANGAN	PERANAN
5.7.1	**Perisikan Ancaman** Maklumat berkaitan ancaman keselamatan maklumat yang berpotensi atau memberi ancaman kepada fungsi USIM perlu diperoleh dan dianalisis untuk menghasilkan maklumat perisikan berkaitan ancaman. Maklumat tentang ancaman sedia ada atau baharu akan dikumpul dan dianalisis untuk memudahkan tindakan dan mengelakkan ancaman atau mengurangkan impak kepada aset maklumat yang terlibat.	CSIRT USIM Pemilik Sistem

ID	KETERANGAN	PERANAN
	(a) Pemilik sistem hendaklah melaksanakan tindakan berikut bagi meningkatkan tahap kawalan keselamatan aset: (b) Mengenal pasti ancaman dengan melaksanakan penilaian risiko terhadap aset maklumat; (c) Mengenal pasti dan melaksanakan kawalan keselamatan yang berkaitan. Kawalan keselamatan tersebut juga dijadikan sebagai satu daripada keperluan dalam kitar hayat pembangunan sistem dan penyediaan infrastruktur ICT; dan (d) Menjadikan ancaman sebagai satu daripada ancaman yang perlu diambil kira dalam pelaksanaan ujian keselamatan sistem dan infrastruktur ICT.	

5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK

ID	KETERANGAN	PERANAN
5.8.1	**Keselamatan Maklumat dalam Pengurusan Projek** Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek tanpa mengira kerumitan, saiz, tempoh serta bidang. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek USIM; (b) Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; (c) Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan;	Ketua Projek Pengurus Projek Pemilik Sistem Pengguna

ID	KETERANGAN	PERANAN
	(d) Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan siber; (e) Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan **pasukan projek pihak pembekal mempunyai pensijilan keselamatan maklumat**;	

ID	KETERANGAN	PERANAN
5.8.2	**Analisis dan Spesifikasi Keperluan Keselamatan Maklumat (*Information Security Requirements Analysis and Specifications*)** Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada serta mematuhi perkara-perkara berikut: (a) Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk pengkonsepan perisian, kajian	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penyelenggaraan dan pelupusan; (b) Semua sistem yang dibangunkan sama ada secara dalaman atau khidmat luar hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan PKS USIM; (c) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan (d) Ujian keselamatan perlu dilakukan semasa pembangunan sistem seperti Pengekodan Selamat (*Secure Coding*) bagi memastikan kesahihan dan integriti data. (e) Penilaian Tahap Keselamatan (*Security Posture Assessment*, SPA) hendaklah dilaksanakan selaras dengan keperluan semasa USIM.	

5.9 INVENTORI MAKLUMAT DAN ASET LAIN YANG BERKAITAN

ID	KETERANGAN	PERANAN
5.9.1	**Inventori Aset** Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT Universiti. Tanggungjawab yang perlu dipatuhi merangkumi perkara yang berikut: (a) Ketua PTJ hendaklah mengenal pasti Pegawai Penerima Aset setiap di setiap Jabatan/Pusat untuk mengurus penerimaan aset-aset ICT bagi projek-projek ICT; (b) Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumentasikan, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemas kini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa; (c) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pegawai yang dibenarkan sahaja; (d) Memastikan inventori maklumat dan aset lain yang berkaitan hendaklah tepat, terkini, dan konsisten; dan (e) Pegawai Aset hendaklah mengesahkan penempatan aset ICT.	Ketua PTJ, Pegawai Aset/Penerima Aset, Pengguna

ID	KETERANGAN	PERANAN
5.9.2	**Pemilikan Aset** Aset yang diselenggara hendaklah hak milik USIM. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut: (a) Memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset; (b) Memastikan aset telah dikelaskan dan dilindungi; (c) Kenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan; (d) Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapuskan atau dilupuskan; (e) Memastikan semua jenis aset dipelihara dengan baik.	Pegawai Aset, Staf USIM

ID	KETERANGAN	PERANAN
5.9.3	**Pengelasan Maklumat Aset** Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan.	Pegawai Pengelas

5.10 PENGGUNAAN MAKLUMAT YANG BOLEH DITERIMA DAN ASET LAIN YANG BERKAITAN

ID	KETERANGAN	PERANAN
5.10.1	**Penggunaan Aset yang Dibenarkan** Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.	Pemilik Aset

5.10.2	**Pengendalian Aset** Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah perlu mengambil kira langkah-langkah keselamatan berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa dan menentukan maklumat adalah tepat dan lengkap dari semasa ke semasa; (c) Menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan; (g) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum; (h) Sekatan capaian yang menyokong keperluan perlindungan untuk setiap	Staf USIM dan pengguna

ID	KETERANGAN	PERANAN
	peringkat pengelasan; dan (i) Penyelenggaraan rekod pengguna yang dibenarkan bagi maklumat dan aset lain yang berkaitan.	

5.11 PEMULANGAN ASET

ID	KETERANGAN	PERANAN
5.11.1	**Pemulangan Aset** Pengguna perlu mengembalikan aset termasuk semua aset lain yang berkaitan seperti peranti storan mudah alih, peranti pengguna fizikal yang disambungkan kepada sistem rangkaian, salinan maklumat fizikal dan perkakasan pengesahan (contohnya token fizikal dan kad pintar) untuk sistem maklumat, tapak serta arkib fizikal mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan atau penamatan perkhidmatan atau kontrak. Pemulangan aset yang mengandungi maklumat rasmi USIM hendaklah disanitasi mengikut Garis Panduan ICT yang diguna pakai.	Staf USIM

5.12 PENGELASAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.12.1	**Pengelasan Maklumat** Pengelasan maklumat terdiri daripada aktiviti penentuan klasifikasi maklumat serta penentuan peringkat keselamatan maklumat. Klasifikasi maklumat terdiri daripada maklumat rahsia rasmi dan maklumat rasmi manakala peringkat keselamatan maklumat terdiri daripada rahsia besar, rahsia, sulit, terhad, data terkawal/sensitif dan terbuka. Data dan maklumat bagi dokumen rahsia rasmi perlu dikelas oleh Pegawai Pengelas mengikut keperluan keselamatan maklumat yang telah ditetapkan dalam Arahan Keselamatan (Semakan dan Pindaan 2017) berdasarkan keperluan perlindungan keselamatan maklumat tersebut. Bagi dokumen rasmi, penentuan berkaitan pengurusan, penggunaan dan pengendalian data serta maklumat dokumen tersebut hendaklah dirujuk kepada Pegawai yang diberi kuasa atau Pegawai yang bertanggungjawab terhadap sesuatu urusan berkenaan.	Pegawai Pengelas

ID	KETERANGAN	PERANAN
	Perkara di bawah hendaklah dilaksanakan oleh semua pihak yang terlibat dalam pengelasan maklumat: (a) Maklumat/dokumen rahsia rasmi hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik oleh Menteri melalui suatu perakuan di bawah tandatangannya dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan dalam Arahan Keselamatan (Semakan dan Pindaan 2017); (b) Mematuhi piawaian, prosedur, tatacara dan garis panduan keselamatan dan pengendalian maklumat atau dokumen yang sedang berkuat kuasa; (c) Memberi perhatian semasa mengendalikan maklumat terutama dokumen yang mengandungi rahsia rasmi; (d) Memastikan tiada pendedahan maklumat kepada pihak yang tidak dibenarkan; (e) Pengelasan maklumat hendaklah berpandukan kepada Akta Rahsia Rasmi 1972, Arahan Keselamatan	

ID	KETERANGAN	PERANAN
	(Semakan dan Pindaan 2017), Pekeliling Am Bilangan 2 Tahun 1987 Garis Panduan Mengenai Pengelasan Fail; (f) Pengurusan maklumat dan rekod hendaklah berpandukan kepada Akta Arkib Negara 2003, Pekeliling Am Bilangan 5 Tahun 2007 – Pengurusan Rekod Awam, Arahan Keselamatan (Semakan dan Pindaan 2017) dan standard berkaitan pengurusan rekod serta pekeliling, arahan, dasar, dan garis panduan yang dikeluarkan oleh Pejabat Pegawai Keselamatan Kerajaan dan Arkib Negara Malaysia; dan (g) Memastikan kesemua fail fizikal dan digital maklumat disimpan mengikut keperluan perlindungan keselamatan yang ditetapkan oleh pihak Kerajaan. Selain keperluan pengelasan dan penentuan peringkat keselamatan maklumat, sebarang maklumat yang mengandungi data peribadi hendaklah diurus dan diproses dengan mematuhi Akta Perlindungan Data Peribadi 2010 [Akta 709], setakat yang terpakai,	

ID	KETERANGAN	PERANAN
	merangkumi keseluruhan kitar hayat data termasuk pengumpulan, penggunaan, penyimpanan, penyelenggaraan, akses, pendedahan, perkongsian, pemindahan, pengarkiban dan pelupusan. Bagi perkara berkaitan perlindungan dan pengurusan data peribadi, pihak yang berkenaan hendaklah merujuk kepada Pegawai Perlindungan Data (Data Protection Officer – DPO) USIM yang telah dilantik mengikut keperluan.	

5.13 PELABELAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.13.1	**Pelabelan Maklumat** Peringkat keselamatan bagi dokumen rahsia rasmi hendaklah ditandakan mengikut klasifikasi dokumen yang kekal terjilid dengan huruf cerai atau huruf besar tidak kurang daripada 7mm di sebelah luar kulit hadapan dan belakang, di muka tajuk, di muka surat pertama dan penghabisan. Peringkat keselamatan hendaklah juga ditanda dengan huruf cerai atau dicap dengan huruf besar di penjuru kiri sebelah atas dan di penjuru kanan sebelah bawah di setiap muka surat yang mengandungi perkara bertulis, bercetak atau bercap.	Staf USIM

ID	KETERANGAN	PERANAN
	Peringkat keselamatan bagi dokumen rahsia rasmi yang tidak kekal terjilid pula hendaklah dicap, ditaip atau ditulis dengan huruf besar di penjuru kiri sebelah atas dan di penjuru kanan sebelah bawah tiap-tiap muka surat yang mengandungi perkara bertulis, bercetak atau bercap. Bagi maklumat/dokumen jenis lukisan, tekapan, negatif foto dan gambar foto yang merupakan rahsia rasmi hendaklah ditandakan peringkat keselamatan supaya peringkatnya dapat dilihat pada salinan yang dibuat daripadanya. Sebagai tambahan, peringkat keselamatan juga hendaklah ditandakan di sebelah belakang jika ia bercetak. Selain daripada itu, bagi sistem aplikasi yang menyimpan maklumat rahsia rasmi perlulah berupaya untuk memberikan tanda keselamatan pada setiap antara muka (*interface*) dan juga pada semua janaan dengan ciri-ciri keselamatan yang bersesuaian dengan peringkat keselamatan dan penilaian risiko. Semua maklumat yang ditandakan sebagai rahsia rasmi hendaklah mematuhi	

ID	KETERANGAN	PERANAN
	Arahan Keselamatan (Semakan dan Pindaan 2017): Keselamatan Rahsia Rasmi (Bab 4) dan semua maklumat yang diklasifikasikan rahsia rasmi dalam format digital/elektronik hendaklah mematuhi Arahan Keselamatan (Semakan dan Pindaan 2017): Keselamatan Rahsia Rasmi dalam Persekitaran Teknologi Maklumat dan Komunikasi (ICT) (Bab 5). Selain pelabelan maklumat peringkat keselamatan bagi dokumen rahsia rasmi, pelabelan maklumat yang mengandungi data peribadi juga hendaklah dibuat dan dikendalikan mengikut keperluan perlindungan data peribadi selaras dengan Akta Perlindungan Data Peribadi 2010 [Akta 709] dan ketetapan dalam Memo Dalaman USIM bertarikh 1 Julai 2026. Sebarang perkara berkaitan pelabelan dan perlindungan data peribadi hendaklah dirujuk kepada Pegawai Perlindungan Data (Data Protection Officer – DPO) USIM yang telah dilantik.	

5.14 PEMINDAHAN DATA DAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.14.1	**Polisi dan Prosedur Pemindahan Data dan Maklumat** Memastikan keselamatan perpindahan/pertukaran data, maklumat dan perisian antara USIM dan pihak luar terjamin. Pihak luar ialah pihak yang menggunakan atau pihak yang membekalkan data, maklumat atau perisian.	Pengguna, warga USIM, pembekal

ID	KETERANGAN	PERANAN
	Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; (b) Terma pemindahan data, maklumat dan perisian antara Universiti dengan pihak luar hendaklah dimasukkan dalam perjanjian pertukaran data, maklumat atau perisian; (c) Media yang mengandungi data, maklumat dan perisian perlu dilindungi; dan (d) Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.	

ID	KETERANGAN	PERANAN
5.14.2	**Perjanjian Mengenai Pemindahan Data dan Maklumat** Semua pihak yang terlibat perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara Universiti dengan pihak luar. Perkara yang perlu dipertimbangkan ialah: (a) Pengarah SDEC hendaklah mengawal penghantaran dan penerimaan data atau maklumat USIM; (b) Mewujudkan prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat USIM; (c) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan (d) Mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.	CDO Pengarah SDEC Warga USIM

5.14.3	**Pesanan Elektronik** Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik dan undang-undang bertulis lain yang berkuat kuasa adalah seperti LAMPIRAN B: (a) Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan Bilangan 1 Tahun 2003 (b) Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 – Pematuhan Tatacara Penggunaan E-mel dan Internet; (c) Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 - Langkah-langkah mengenai penggunaan Mel Elektronik Agensi-agensi Kerajaan; (d) Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan Government Unified Communication (MyGovUC) dan mana-mana undang-undang bertulis yang berkuat kuasa; dan (e) Sebarang e-mel rasmi hendaklah disimpan untuk tujuan rekod.	Warga USIM

5.15 KAWALAN CAPAIAN

ID	KETERANGAN	PERANAN
5.15.1	**Polisi Kawalan Capaian** Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Kawalan capaian perlu disemak, dikemas kini dan disahkan **sekurang-kurangnya sekali dalam tempoh setahun** atau mengikut keperluan sekiranya terdapat perubahan serta menyokong peraturan kawalan capaian pengguna sedia ada. Perkara-perkara yang perlu dipertimbangkan dalam menentukan kawalan capaian ialah seperti yang berikut: (a) Menentukan entiti mana yang memerlukan jenis capaian kepada maklumat dan aset lain yang berkaitan; (b) Keperluan keselamatan aplikasi ditentukan dan diselaraskan dengan keperluan capaian entiti; (c) Hak capaian dan dasar klasifikasi maklumat sistem dan rangkaian; (d) Capaian fizikal, yang perlu disokong	Pemilik Sistem Pentadbir Sistem ICT.

ID	KETERANGAN	PERANAN
	oleh kawalan kemasukan fizikal yang sesuai; (e) Penyebaran maklumat dan kebenaran capaian perlu mematuhi prinsip-prinsip keselamatan yang ditetapkan dan mengikut pengelasan maklumat; (f) Sekatan kepada capaian istimewa hendaklah dihadkan dan diurus (pengurusan hak capaian); (g) Pengasingan tugas, fungsi kawalan capaian (contohnya permintaan capaian, kebenaran capaian, pentadbiran capaian); (h) Patuh undang-undang, peraturan berkaitan yang berkuat kuasa semasa dan sebarang kewajipan kontrak berkaitan pengehadan capaian kepada data atau perkhidmatan; (i) Kebenaran rasmi untuk permintaan capaian; (j) Kebenaran rasmi permohonan capaian; (k) Hak capaian istimewa; dan (l) Pengelogan aktiviti yang dilaksanakan.	

ID	KETERANGAN	PERANAN
5.15.2	**Capaian kepada Rangkaian dan Perkhidmatan Rangkaian** Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari USIM. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang aset maklumat dan perkakasan ICT yang bersesuaian antara rangkaian USIM, rangkaian agensi lain dan rangkaian awam; (b) Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO, Pengarah SDEC

ID	KETERANGAN	PERANAN
5.15.3	**Kawalan Capaian** Kawalan capaian adalah untuk mengurus, mengawasi, dan meningkatkan capaian maklumat dan aset maklumat dengan selamat. Ini merangkumi pelbagai aspek operasi dan pengurusan untuk memastikan mencapai matlamat, sasaran, dan hasil yang diinginkan dengan kawalan seperti yang berikut: (a) Mematuhi undang-undang, peraturan, dan polisi yang berkaitan dengan keselamatan maklumat; (b) Memastikan bahawa dasar, prosedur, dan amalan keselamatan maklumat diikuti dan dilaksanakan dengan betul; (c) Mengenal pasti, menilai, dan menguruskan risiko keselamatan maklumat yang berkaitan dengan operasi dan capaian maklumat universiti; (d) Memastikan keselamatan maklumat dan data dalam universiti dengan mematuhi amalan keselamatan maklumat yang sesuai; (e) Meningkatkan kesedaran dan kefahaman kakitangan tentang peningkatan capaian dan amalan	Pentadbir Sistem Pentadbir Aset

ID	KETERANGAN	PERANAN
	keselamatan dalam universiti; dan (f) Memantau dan menilai prestasi keselamatan capaian berterusan untuk mengenal pasti peningkatan dan kesan tindakan yang diperlukan.	

ID	KETERANGAN	PERANAN
5.15.4	**Keperluan Pemindahan Maklumat** Menghadkan capaian pembekal, kakitangan dan pengguna pihak luar kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat. Memastikan dokumen perjanjian diwujudkan antara USIM dengan pihak ketiga bagi pemindahan maklumat melibatkan pihak ketiga.	

5.16 PENGURUSAN IDENTITI

ID	KETERANGAN	PERANAN
5.16.1	**Pendaftaran dan Pembatalan Pengguna** Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara–perkara berikut hendaklah dipatuhi: (a) Akaun pengguna hanya diwujudkan setelah mendapat status pengesahan daripada sumber data atau Pemilik Sistem dan pengguna telah membuat perakuan pematuhan PKS USIM melalui Surat Akuan Pematuhan Polisi Keselamatan Siber seperti **LAMPIRAN A.** (b) Akaun yang diperuntukkan kepada pengguna sahaja boleh digunakan; (c) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (d) Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada USIM terlebih dahulu;	Warga USIM

ID	KETERANGAN	PERANAN
	(e) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan USIM; (f) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan semua pengguna tertakluk kepada peraturan yang ditetapkan. (g) Penggunaan akaun milik individu lain **DILARANG**; (h) Akaun pengguna tidak boleh dikongsi; (i) Akaun pengguna boleh dibekukan atau ditamatkan apabila menerima arahan daripada Bahagian Pengurusan Sumber Manusia atas sebab-sebab yang berikut: (i) Bertukar bidang tugas kerja; (ii) Bertukar ke Universiti lain; (iii) Bersara; (iv) Bagi menjalankan siasatan; atau (v) Ditamatkan perkhidmatan. (j) Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Semua capaian ini perlu direkodkan, dikemas kini dan menyokong polisi kawalan capaian pengguna sedia ada.	

ID	KETERANGAN	PERANAN
5.16.2	**Pengurusan Identiti** Pengurusan akaun pengguna bagi capaian ke sistem atau aset maklumat bermula daripada penciptaan rekod pengguna baharu sehingga penamatan profil apabila pengguna telah meletakkan jawatan, bersara atau meninggal dunia dalam perkhidmatan. Pendaftaran, pengemaskinian dan penamatan akaun pengguna dilaksanakan mengikut prosedur yang ditetapkan. Proses pengurusan akaun pengguna harus memastikan bahawa: (a) Identiti yang diberikan khusus hanya dikaitkan dengan seorang sahaja untuk membolehkan orang itu bertanggungjawab atas tindakan yang dilakukan dengan identiti khusus ini; (b) Akaun pengguna akan dinyahaktifkan selaras dengan perubahan status daripada sumber data; dan (c) Log penggunaan dan pengurusan identiti pengguna dan maklumat pengesahan hendaklah disimpan.	Warga USIM, Pentadbir Sistem

5.17 MAKLUMAT PENGESAHAN IDENTITI

ID	KETERANGAN	PERANAN
5.17.1	**Pengurusan Maklumat Pengesahan Identiti Pengguna** Peruntukan maklumat pengesahan identiti pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan. Peruntukan dan proses pengurusan hendaklah memastikan bahawa: (a) Prosedur yang telah diwujudkan untuk mengesahkan identiti pengguna sebelum memberikan maklumat pengesahan baharu, gantian atau sementara; (b) Maklumat pengesahan, termasuk maklumat pengesahan sementara, dihantar kepada pengguna secara selamat (contohnya, melalui saluran yang disahkan dan dilindungi), dan penggunaan mesej e-mel elektronik yang tidak dilindungi (clear text) untuk tujuan ini hendaklah dielakkan;	Pengguna Sistem, Pentadbir Sistem

ID	KETERANGAN	PERANAN
	(c) Pengguna mengakui penerimaan maklumat pengesahan identiti pengguna; (d) Maklumat pengesahan tetapan asal (*default*) seperti yang ditetapkan atau diberikan oleh sistem diubah dengan segera selepas pemasangan sistem, perkakasan atau perisian; (e) Rekod peristiwa penting mengenai peruntukan dan pengurusan maklumat pengesahan identiti pengguna disimpan dan kerahsiaannya dijamin, serta kaedah penyimpanan rekod disetujui (contohnya dengan menggunakan alat penyimpanan kata laluan yang diluluskan).	

ID	KETERANGAN	PERANAN
5.17.2	**Penggunaan Maklumat Pengesahan Rahsia** Peranan dan tanggungjawab pengguna ialah seperti yang berikut: (a) Membaca, memahami dan	Pengguna, Pentadbir Sistem ICT, Pengarah SDEC

ID	KETERANGAN	PERANAN
	mematuhi PKS USIM; (b) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya; (c) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat USIM; (d) Melaksanakan langkah-langkah perlindungan seperti yang 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 yang ditetapkan; (vi) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (vii) Menjaga kerahsiaan	

ID	KETERANGAN	PERANAN
	langkah-langkah keselamatan siber daripada diketahui umum. (e) Maklumat pengesahan terjejas atau telah dikompromi hendaklah diubah serta-merta melibatkan sekatan akses, perubahan polisi dan kata laluan apabila pemberitahuan atau petunjuk sebarang kompromi diterima; (f) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CSIRT USIM dengan segera; (g) Menghadiri program-program kesedaran mengenai keselamatan siber; (h) Tidak dibenarkan menyebarkan maklumat universiti di dalam sebarang platform digital melainkan dengan kebenaran; dan (i) Pengguna perlu mengikut amalan keselamatan yang baik dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti pengguna.	

ID	KETERANGAN	PERANAN
5.17.3	**Sistem Pengurusan Kata Laluan** Sistem pengurusan kata laluan hendaklah interaktif dan mengambil kira kualiti kata laluan yang dicipta. Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh universiti seperti yang berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan **tidak boleh dikongsi** dengan sesiapa pun; (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi bagi sistem yang menyokong *Multi-Factor Authentication* (MFA). Bagi sistem yang tidak menyokong *Multi-Factor Authentication* (MFA), kata laluan hendaklah ditukar sekurang-kurangnya dalam tempoh **enam bulan sekali**; (c) Panjang kata laluan mestilah sekurang-kurangnya **8 AKSARA** dengan gabungan antara huruf, aksara khas dan nombor (alphanumeric) KECUALI bagi	Pengguna, Pentadbir Sistem, ICTSO, Pengarah SDEC

ID	KETERANGAN	PERANAN
	perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; (d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekali pun; (e) Kata laluan kunci skrin (*lock screen*) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara; (g) Kuatkuasakan pertukaran kata laluan semasa atau selepas login kali pertama atau selepas reset kata laluan; (h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna (i) 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	

ID	KETERANGAN	PERANAN
	(j) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	

5.18 HAK CAPAIAN (*Access Rights*)

ID	KETERANGAN	PERANAN
5.18.1	**Peruntukan Capaian Pengguna** Hak capaian kepada maklumat dan aset maklumat yang berkaitan hendaklah diperuntukkan, disemak, diubah suai dan dikeluarkan mengikut dasar/peraturan atau garis panduan kawalan capaian yang berkuat kuasa. Pentadbir Sistem ICT perlu mewujudkan prosedur pendaftaran dan penamatan pengguna sistem masing-masing. Proses peruntukan capaian pengguna dan pembatalan hak capaian fizikal dan logik yang diberikan kepada entiti yang telah disahkan identitinya hendaklah termasuk: (a) Hak Capaian yang berkaitan dengan	Pentadbir Sistem ICT, Pengurus Projek, Pembekal, Pihak yang mempunyai urusan dengan perkhidmatan ICT USIM

ID	KETERANGAN	PERANAN
	setiap sistem atau produk yang perlu diberikan hendaklah dikenal pasti dan dibenarkan. (b) Hak capaian maklumat dan aset maklumat mesti dihadkan berdasarkan keperluan untuk mengetahui dan prinsip-prinsip keselamatan yang ditetapkan; (c) Individu yang bukan warga USIM **TIDAK boleh diberikan** ID pengguna atau diberi keistimewaan untuk menggunakan atau mencapai aset (komputer, maklumat atau sistem komunikasi) melainkan setelah mendapat kebenaran USIM; (d) Kebenaran rasmi mestilah telah ditandatangani oleh wakil yang diberi kuasa di pihak ketiga sebelum capaian diberikan kepada mana-mana pihak ketiga (pihak syarikat);	

ID	KETERANGAN	PERANAN
	(e) Hak capaian hendaklah ditamatkan apabila entiti/individu tidak lagi perlu mencapai maklumat dan aset maklumat yang berkaitan tepat pada masanya; (f) Hak capaian sementara untuk tempoh masa terhad boleh dipertimbangkan bila diperlukan dan hendaklah dibatalkan pada tarikh tamat tempoh; (g) Tahap capaian yang diberikan hendaklah mengikut dasar kawalan capaian yang ditetapkan, peranan dan konsisten dengan keperluan keselamatan maklumat lain seperti pengasingan tugas; (h) Hak capaian pengguna hendaklah diubah suai selari dengan peranan atau pekerjaan; (i) Hak capaian diaktifkan hanya selepas kebenaran diperoleh; dan (j) Rekod hak capaian logik dan fizikal pengguna hendaklah disimpan.	

ID	KETERANGAN	PERANAN
5.18.2	**Kajian Semula Hak Capaian Pengguna** Pentadbir sistem hendaklah menyemak hak capaian pengguna secara berkala sekurang-kurangnya **sekali dalam tempoh setahun**. Pentadbir Sistem perlu mewujudkan rekod pendaftaran dan penamatan pengguna sistem masing-masing sebagai rujukan semakan ke atas hak capaian pengguna secara berkala. Semakan ke atas hak capaian fizikal dan logik harus mempertimbangkan perkara berikut: (a) Hak capaian pengguna selepas sebarang perubahan dalam universiti (contohnya pertukaran pekerjaan, kenaikan pangkat, penurunan pangkat) atau penamatan perkhidmatan/pekerjaan; dan (b) Kebenaran untuk hak capaian istimewa.	Pentadbir Sistem, Pengurus Projek, Pembekal, Pihak yang mempunyai urusan dengan perkhidmatan ICT USIM

ID	KETERANGAN	PERANAN
5.18.3	**Pembatalan atau Pelarasan Hak Capaian** Hak akses kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam USIM.	Pentadbir Sistem ICT, Pengarah SDEC

ID	KETERANGAN	PERANAN
5.18.4	**Tanggungjawab Pengguna** Memastikan pengguna sistem atau aset maklumat bertanggungjawab melindungi maklumat pengesahan identiti mereka.	Warga USIM, Pembekal, Pihak yang mempunyai urusan dengan perkhidmatan ICT USIM

5.19 KESELAMATAN MAKLUMAT DALAM HUBUNGAN DENGAN PEMBEKAL

ID	KETERANGAN	PERANAN
5.19.1	**Polisi Keselamatan Siber untuk Hubungan dengan Pembekal** Keperluan keselamatan maklumat hendaklah ditakrifkan, dilaksanakan, dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset maklumat. Perkara yang perlu dipertimbangkan ialah seperti yang berikut: (a) Mengenal pasti dan mendokumentasi maklumat pembekal; (b) Menyediakan prosedur pengurusan pembekal termasuk kaedah penilaian mutu perkhidmatan; (c) Memilih pembekal mengikut klasifikasi maklumat dan perkhidmatan yang disediakan oleh pembekal selaras dengan dasar dan peraturan yang berkuat kuasa; (d) Mengawal dan memantau capaian pembekal; (e) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam dokumen perjanjian; (f) Jenis-jenis obligasi kepada pembekal;	Pengarah SDEC Pengurus Projek Pembekal

	(g) Pelan kontingensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; (h) Melaksanakan program kesedaran terhadap PKS USIM kepada pembekal; (i) Menandatangani Surat Setuju Terima; dan (j) Membuat akuan pematuhan PKS USIM; (k) Pembekal perlu mematuhi arahan keselamatan yang sedang berkuat kuasa; dan (l) Mengenal pasti dan melaksanakan proses dan prosedur bagi mengurus risiko yang berkaitan dengan penggunaan produk dan perkhidmatan pembekal termasuk penamatan penggunaan produk dan perkhidmatan pembekal. Pemilik perkhidmatan atau projek hendaklah memastikan proses penamatan pembekal yang selamat, termasuk: (a) membatalkan peruntukan hak capaian; (b) pengendalian maklumat; (c) menentukan pemilikan harta intelek yang dibangunkan semasa perjanjian dilaksanakan;	

ID	KETERANGAN	PERANAN
	(d) mudah alih maklumat sekiranya berlaku pertukaran pembekal atau penyumberan; (e) pengurusan rekod; (f) pemulangan aset; (g) pelupusan selamat maklumat dan aset lain yang berkaitan; dan (h) keperluan kerahsiaan berterusan.	

5.20 MENANGANI KESELAMATAN DALAM PERJANJIAN DENGAN PEMBEKAL

ID	KETERANGAN	PERANAN
5.20.1	**Menangani Keselamatan Dalam Perjanjian Pembekal** Semua keperluan keselamatan maklumat yang berkaitan hendaklah ditakrifkan, disediakan dan dipersetujui dengan setiap pembekal yang boleh mencapai, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak USIM selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.	Syarikat Pembekal

	Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Syarikat pembekal hendaklah mempunyai pendaftaran sah dengan Universiti; (b) Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; (c) Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada Universiti berkaitan; (d) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; (e) Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal; (f) Laporan penilaian pihak ketiga yang	

ID	KETERANGAN	PERANAN
	dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut: (i) Badan penilai pihak ketiga adalah bebas dan berintegriti; (ii) Badan penilai pihak ketiga adalah kompeten; (iii) Kriteria penilaian; (iv) Parameter pengujian; dan (v) Andaian yang dibuat berkaitan dengan skop penilaian. (g) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan USIM; dan (h) Pembekal hendaklah mematuhi pengelasan maklumat yang telah ditetapkan oleh USIM.	

5.21 MENGURUS KESELAMATAN MAKLUMAT DALAM RANGKAIAN BEKALAN ICT

ID	KETERANGAN	PERANAN
5.21.1	**Rantaian Bekalan Teknologi Maklumat dan Komunikasi** 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 ialah seperti yang berikut: (a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; (b) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan (c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	Pengarah SDEC, Pembekal, Pemilik Projek

5.22 MEMANTAU, MENYEMAK DAN MENGURUS PERUBAHAN PERKHIDMATAN PEMBEKAL

ID	KETERANGAN	PERANAN
5.22.1	**Memantau dan Mengkaji Semula Perkhidmatan Pembekal** USIM hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: (a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; (b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan (c) Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	Pengarah SDEC, Pembekal, Pemilik Projek

ID	KETERANGAN	PERANAN
5.22.2	**Menguruskan Perubahan Kepada Perkhidmatan Pembekal (*Managing Changes to Supplier Services*)** Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diurus dengan mengambil kira kepentingan maklumat, sistem dan perkhidmatan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira ialah seperti yang berikut: (a) Perubahan dalam perjanjian dengan pembekal; (b) Perubahan yang dilakukan oleh Universiti bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan (c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	Pengarah SDEC, Pembekal, Pemilik Projek

5.23 KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN PENGKOMPUTERAN AWAN

ID	KETERANGAN	PERANAN
5.23.1	**Keselamatan maklumat bagi penggunaan perkhidmatan pengkomputeran awan** Pengurusan perkhidmatan awan ini melibatkan pelbagai aspek teknikal dan pentadbiran untuk memastikan perkhidmatan awan digunakan secara berkesan, selamat, dan sesuai dengan keperluan universiti. Perkara berikut perlu dipatuhi oleh semua pihak yang terlibat: (a) Memastikan kepatuhan terhadap keperluan perundangan, peraturan, garis panduan dan perjanjian kontrak yang berkaitan. (b) Pengurusan perkhidmatan yang disediakan oleh pembekal yang dilantik oleh pihak universiti; (c) Menentukan/mentakrifkan dan memaklumkan cara/kaedah berkaitan pengurusan risiko bagi perkhidmatan pengkomputeran awan;	Pentadbir Sistem

ID	KETERANGAN	PERANAN
	(a) Memastikan keperluan keselamatan maklumat yang berkaitan dengan penggunaan perkhidmatan pengkomputeran awan dilaksanakan; dan (b) Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	

5.24 PERANCANGAN DAN PENYEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.24.1	**Tanggungjawab dan Prosedur** Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden USIM adalah berdasarkan kepada Garis Panduan: Pengurusan Pengendalian Insiden Keselamatan ICT USIM yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Memberikan kesedaran berkaitan Garis Panduan: Pengurusan Pengendalian Insiden Keselamatan ICT USIM dan hebahan kepada warga USIM sekiranya ada perubahan; dan (b) Memastikan personel yang mengurus insiden mempunyai tahap kompetensi yang diperlukan.	ICTSO, Pengarah SDEC, CSIRT USIM, Pemilik Projek/Sistem Aplikasi

5.25 PENILAIAN DAN KEPUTUSAN MENGENAI KEJADIAN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.25.1	**Penilaian dan Keputusan Mengenai Peristiwa Keselamatan Maklumat** Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.	ICTSO

5.26 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.26.1	**Tindak Balas Terhadap Insiden Keselamatan** Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT USIM. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut:	ICTSO, CSIRT USIM

ID	KETERANGAN	PERANAN
	(a) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; (b) Menjalankan kajian forensik sekiranya perlu; (c) Menghubungi pihak yang berkenaan dengan secepat mungkin; (d) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti; (e) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (f) Menyediakan pelan kontigensi dan sekiranya perlu mengaktifkan pelan kesinambungan perkhidmatan; (g) Menyediakan tindakan pemulihan segera; dan (h) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu	

5.27 PENGAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.27.1	**Pembelajaran Daripada Insiden Keselamatan Maklumat** Pengetahuan yang diperoleh daripada penganalisisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya. 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. Maklumat yang diperoleh daripada penilaian insiden keselamatan maklumat hendaklah digunakan untuk:	ICTSO, CSIRT USIM

ID	KETERANGAN	PERANAN
	(a) mempertingkat pelan pengurusan insiden termasuk senario dan prosedur insiden; (b) mengenal pasti insiden berulang atau serius dan puncanya untuk mengemas kini penilaian risiko keselamatan maklumat universiti dan menentukan serta melaksanakan kawalan tambahan yang diperlukan untuk mengurangkan kemungkinan atau akibat kejadian serupa pada masa hadapan. Mekanisme untuk membolehkan itu termasuk mengumpul, mengukur dan memantau maklumat tentang jenis insiden, kekerapan insiden serta kos yang terlibat; dan (c) meningkatkan kesedaran dan latihan pengguna dengan memberikan contoh tentang perkara yang boleh berlaku, cara bertindak balas terhadap insiden tersebut dan cara mengelak pada masa hadapan.	

5.28 PENGUMPULAN BAHAN BUKTI

ID	KETERANGAN	PERANAN
5.28.1	**Pengumpulan Bahan Bukti** USIM hendaklah menentukan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.	ICTSO, CSIRT USIM

5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN

ID	KETERANGAN	PERANAN
5.29.1	**Keselamatan Maklumat Semasa Gangguan** Keselamatan maklumat semasa gangguan merujuk kepada langkah-langkah dan prosedur yang diambil untuk melindungi dan mengekalkan keselamatan maklumat, data, dan sistem ICT semasa terjadi gangguan, bencana atau insiden yang boleh mengancam integriti dan ketersediaan maklumat. Gangguan ini termasuk pelbagai situasi seperti serangan siber, bencana alam, kebakaran, banjir, kecurian, atau insiden teknikal yang tidak diingini. Aspek penting berkaitan dengan keselamatan maklumat semasa gangguan yang perlu diberi perhatian ialah seperti yang berikut:	Koordinator PKP, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan Bencana ICT

	(a) Pembangunan dan pelaksanaan Pelan Perancangan Kesinambungan Perkhidmatan (*Business Continuity Planning*) untuk memastikan penyampaian perkhidmatan USIM berfungsi dengan minimum gangguan ketika terjadi insiden; (b) Pemulihan Bencana melibatkan pelan dan tindakan untuk memulihkan sistem maklumat dan data setelah bencana atau insiden; (c) Perlindungan Data melibatkan salinan data secara berkala, pengekalan data yang baik, dan pelaksanaan tindakan keselamatan yang sesuai untuk melindungi data terperingkat; (d) Pencegahan Serangan Siber (*Cybersecurity Measures*) melibatkan tindakan untuk mencegah serangan siber dan melindungi data daripada ancaman siber; (e) Proses pemulihan adalah berdasarkan keutamaan merujuk kepada dokumen DRP untuk mengurangkan masa henti ketika terjadi gangguan; (f) Kawalan fizikal ke pusat data dan peralatan komputer terhad kepada	

ID	KETERANGAN	PERANAN
	individu yang sah untuk mencegah capaian yang tidak dibenarkan; (g) Pemulihan data memastikan keupayaan untuk memulihkan data yang hilang atau terjejas dalam insiden; (h) Kesedaran keselamatan (*Security Awareness*) untuk mengurangkan ancaman dalaman dan mencegah insiden yang disebabkan oleh kesalahan manusia; (i) Pelan Komunikasi Krisis (*Crisis Communication Plan*) yang jelas untuk mengurus krisis dan insiden dengan pantas. Keselamatan maklumat semasa gangguan ialah aspek penting dalam perancangan keselamatan dan keselamatan data, yang memastikan universiti mampu menjaga integriti, kerahsiaan, dan ketersediaan maklumat penting dalam pelbagai situasi yang mengancam.	

5.30 KESEDIAAN ICT BAGI KESINAMBUNGAN PERKHIDMATAN

ID	KETERANGAN	PERANAN
5.30.1	**Kesinambungan Keselamatan Maklumat** Kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan bisnes Universiti.	ICTSO

5.30.2	**Perancangan Kesinambungan Keselamatan Maklumat** USIM hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, USIM perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi USIM. USIM juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan ialah seperti yang berikut: (a) Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) USIM; (b) Menetapkan polisi PKP; (c) Mengenal pasti perkhidmatan kritikal; (d) Melaksanakan Kajian Impak Perkhidmatan (Business Impact Analysis, BIA) dan Penilaian Risiko terhadap perkhidmatan kritikal; (e) Membangunkan Pelan Induk	Koordinator PKP, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan Bencana ICT

ID	KETERANGAN	PERANAN
	Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT. (f) Melaksanakan program kesedaran dan latihan pasukan PKP dan warga USIM; (g) Melaksanakan simulasi pelan kesinambungan perkhidmatan; dan (h) Melaksanakan kemas kini ke atas pelan kesinambungan perkhidmatan.	

ID	KETERANGAN	PERANAN
5.30.3	**Pelaksanaan Kesinambungan Keselamatan Maklumat** USIM 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 ialah seperti yang berikut: (a) Melaksanakan PKP apabila terdapat	Koordinator PKP, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan Bencana ICT

ID	KETERANGAN	PERANAN
	gangguan terhadap perkhidmatan kritikal Universiti yang telah dikenal pasti berdasarkan kepada Pelan Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak Balas Kecemasan dan Pelan Pemulihan Bencana; (b) Melaksanakan pasca nilai (*post-mortem*) dan mengemas kini pelan-pelan yang terlibat; (c) Mengemas kini pelan-pelan yang terlibat jika berlaku perubahan kepada fungsi kritikal USIM; (d) Mengemas kini struktur tadbir urus PKP USIM sekiranya berlaku pertukaran keahlian pasukan; dan (e) Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP.	

ID	KETERANGAN	PERANAN
5.30.4	**Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat** USIM hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan **sekurang-kurangnya dua tahun sekali** bagi memastikannya terpakai dan berkesan semasa situasi kecemasan. Kesediaan ICT hendaklah dirancang, dilaksanakan, diselenggara dan diuji berdasarkan objektif kesinambungan perniagaan dan keperluan kesinambungan ICT. USIM hendaklah memastikan bahawa: (a) struktur pasukan PKP yang mencukupi disediakan untuk menyediakan, mengurangkan dan bertindak balas terhadap gangguan; (b) Pelan PKP dan pelan-pelan lain yang terlibat termasuk tindak balas dan prosedur pemulihan hendaklah dinilai dan diuji melalui pelaksanaan simulasi **sekurang-kurangnya setahun sekali** serta diluluskan oleh pihak pengurusan; (c) Pelan PKP hendaklah	Pengurusan USIM, Koordinator PKP, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan Bencana ICT, Pemilik Sistem Kritikal dalam PKP, warga USIM

ID	KETERANGAN	PERANAN
	mengandungi perkara seperti yang berikut: (i) spesifikasi prestasi dan kapasiti untuk memenuhi keperluan dan objektif kesinambungan perniagaan seperti yang dinyatakan dalam BIA; (ii) Objektif Masa Pemulihan (RTO) bagi setiap perkhidmatan ICT mengikut keutamaan pemulihan dan prosedur untuk memulihkan komponen tersebut; dan (iii) Objektif Titik Pemulihan (RPO) bagi setiap perkhidmatan ICT mengikut keutamaan pemulihan dan prosedur untuk memulihkan komponen tersebut.	

5.31 KEPERLUAN PERUNDANGAN DAN KONTRAK

ID	KETERANGAN	PERANAN
5.31.1	**Pematuhan Terhadap Keperluan Perundangan dan Kontrak** Meningkat dan memantapkan tahap keselamatan siber bagi mengelakkan pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	Warga USIM Pembekal, Pihak yang terlibat dalam perkhidmatan ICT USIM
5.31.2	**Pengenalpastian Keperluan Undang-Undang dan Kontrak Yang Terpakai** Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga USIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT USIM. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di USIM dan pembekal seperti **LAMPIRAN B.**	Warga USIM, pembekal, pakar runding, pihak yang mempunyai urusan dengan perkhidmatan ICT USIM

ID	KETERANGAN	PERANAN
5.31.3	**Peraturan Kawalan Kriptografi** Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi Melindungi kerahsiaan, integriti dan kesahihan maklumat yang merangkumi data di dalam sistem rangkaian, sistem aplikasi dan pangkalan data. Kunci enkripsi mestilah dilindungi dengan menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan. Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut.	Warga USIM, pembekal, pakar runding, pihak yang mempunyai urusan dengan perkhidmatan ICT USIM

5.32 HAK HARTA INTELEK

ID	KETERANGAN	PERANAN
5.32.1	**Hak Harta Intelek** Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan	Warga USIM, pembekal, pakar runding, pihak yang mempunyai urusan dengan perkhidmatan ICT USIM

5.33 PERLINDUNGAN REKOD

ID	KETERANGAN	PERANAN
5.33.1	**Perlindungan Rekod** Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.	Warga USIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT USIM

5.34 PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI

ID	KETERANGAN	PERANAN
5.34.1	**Privasi dan Perlindungan Maklumat Peribadi** USIM hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.	Warga USIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT USIM

5.35 KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI

ID	KETERANGAN	PERANAN
5.35.1	**Kajian Semula Keselamatan Maklumat Secara Berkecuali** Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	Pengarah SDEC, Pemilik Sistem

5.36 PEMATUHAN DASAR, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.36.1	**Pematuhan Polisi dan Standard Keselamatan** USIM hendaklah membuat kajian semula secara berkala terhadap pematuhan dasar dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian.	CDO Pengarah SDEC Pemilik Sistem
5.36.2	**Kajian Semula Pematuhan Teknikal** USIM hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan komputer.	CDO Pengarah SDEC Pemilik Sistem

ID	KETERANGAN	PERANAN
5.36.3	**Memastikan semua polisi, peraturan, akta dipatuhi dan dilaksana oleh semua peringkat proses perkhidmatan.** Semua warga USIM, pembekal dan pihak yang terlibat dalam perkhidmatan ICT USIM hendaklah mematuhi undang-undang, prosedur, dasar, peraturan yang sedang berkuat kuasa.	ICTSO Pengarah SDEC

5.37 DOKUMENTASI PROSEDUR OPERASI STANDARD

ID	KETERANGAN	PERANAN
5.37.1	**Dokumentasi Prosedur Operasi Standard** Penyedia dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut: (a) Semua prosedur keselamatan siber	Pengarah SDEC, ICTSO, Pentadbir Sistem ICT

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

6 KAWALAN SUMBER MANUSIA

Terdapat lapan kawalan sumber manusia yang terpakai dan perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di USIM. Perincian kawalan sumber manusia seperti di bawah.

6.1 TAPISAN KESELAMATAN

ID	KETERANGAN	PERANAN
6.1.1	**Tapisan Keselamatan (*Security Screening*)** Tapisan keselamatan hendaklah dijalankan terhadap warga Universiti, pembekal, pakar runding dan pihak yang mempunyai urusan	Jabatan Pendaftar, Jabatan Keselamatan, USIM 'Alamiyyah, Pengguna

ID	KETERANGAN	PERANAN
	dengan perkhidmatan ICT USIM yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga Universiti, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Universiti yang terlibat dalam menjamin keselamatan aset maklumat sebelum, semasa dan selepas perkhidmatan; dan (b) Menjalankan tapisan keselamatan untuk warga Universiti, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Universiti yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	

6.2 TERMA DAN SYARAT PERKHIDMATAN

ID	KETERANGAN	PERANAN
6.2.1	**Terma dan Syarat Perkhidmatan** Persetujuan berkontrak dengan Warga USIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di USIM hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab universiti terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi ialah seperti yang berikut: (a) menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga Universiti, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT USIM yang terlibat dalam menjamin keselamatan aset ICT; dan (b) mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Pengguna

6.3 KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
6.3.1	**Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat** Warga USIM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka.	CDO, ICTSO

6.4 PROSES TATATERTIB

ID	KETERANGAN	PERANAN
6.4.1	**Proses Tatatertib** Proses tatatertib yang formal perlu ditentukan dan disampaikan kepada warga Universiti atau pihak berkepentingan terlibat yang lain bagi membolehkan tindakan diambil ke atas pelanggaran keselamatan maklumat yang dilakukan. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut:	Jabatan Undang-Undang (JUU)

ID	KETERANGAN	PERANAN
	(a) Memastikan adanya proses tindakan disiplin dan/atau undang-undang sekiranya berlaku pelanggaran terhadap polisi, perundangan dan peraturan yang ditetapkan oleh USIM; dan (b) Warga USIM yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT USIM.	

6.5 TANGGUNGJAWAB SELEPAS PENAMATAN PERANAN ATAU JAWATAN

ID	KETERANGAN	PERANAN
6.5.1	**Pertukaran atau Penamatan Peranan atau Jawatan** Peranan dan tanggungjawab berkaitan keselamatan maklumat yang masih sah selepas penamatan atau pertukaran perjawatan hendaklah ditentukan, dikuat kuasa dan disampaikan kepada Warga USIM dan semua pihak yang terlibat.	Warga USIM

ID	KETERANGAN	PERANAN
	Semua Warga USIM dan pembekal serta pihak yang terlibat dengan perkhidmatan ICT USIM yang telah tamat peranan atau perkhidmatan perlu mematuhi perkara-perkara berikut: (a) Memastikan semua aset maklumat milik USIM atau kerajaan dikembalikan kepada USIM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (c) Maklumat rasmi dalam aset maklumat tidak dibenarkan dibawa keluar dari USIM.	

ID	KETERANGAN	PERANAN
	Warga USIM yang telah bertukar keluar perkhidmatan atau tamat perkhidmatan hendaklah: (a) Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada USIM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (c) Menyediakan dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.	

6.6 PERJANJIAN KERAHSIAAN ATAU KETAKDEDAHAN

ID	KETERANGAN	PERANAN
6.6.1	**Perjanjian Kerahsiaan atau Ketakdedahan** Syarat-syarat perjanjian kerahsiaan atau ketakdedahan (*non-disclosure agreement*) perlu mengambil kira keperluan universiti dan hendaklah dikenal pasti dan didokumentasi dan ditandatangani oleh Warga USIM dan pihak berkepentingan terlibat yang lain. Pembekal atau pihak berkepentingan yang terlibat dengan perkhidmatan ICT USIM hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.	Ketua PTJ ICTSO Pentadbir Sistem ICT Pengguna Pembekal

6.7 BEKERJA SECARA JARAK JAUH

ID	KETERANGAN	PERANAN
6.7.1	**Bekerja Secara Jarak Jauh** Dasar dan langkah-langkah keselamatan hendaklah dilaksanakan bagi melindungi maklumat yang dicapai, diproses atau disimpan secara jarak jauh. Warga USIM yang bekerja jarak jauh hendaklah: (a) Memastikan keselamatan peranti/perkakasan yang digunakan adalah selamat untuk capaian ke sistem aplikasi dan rangkaian USIM; (b) Memastikan keselamatan maklumat Universiti dipatuhi dan tidak disebarkan kepada pihak ketiga; dan (c) memastikan arahan bekerja dari luar dipatuhi mengikut garis panduan yang ditetapkan.	Warga USIM Jabatan Pendaftar

6.8 PELAPORAN INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
6.8.1	**Pelaporan Insiden Keselamatan Maklumat** Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul dengan segera. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada ICTSO. ICTSO kemudiannya perlu melaporkan kepada CSIRT USIM. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) Maklumat disyaki atau didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses disyaki atau didapati hilang, dicuri atau didedahkan; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh atau pencerobohan, penyelewengan dan insiden yang tidak dijangka.	ICTSO, Pengarah SDEC, CSIRT USIM

ID	KETERANGAN	PERANAN
	Prosedur pelaporan insiden keselamatan siber berdasarkan: (a) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; (b) Surat Pekeliling Am Bil. 4/2022: Pengurusan Dan Pengendalian Insiden Keselamatan Siber Sektor Awam; dan (c) Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT USIM	

7 KAWALAN FIZIKAL

Terdapat 14 kawalan fizikal yang terpakai dan perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di USIM. Perincian kawalan fizikal seperti di bawah.

7.1 PERIMETER KESELAMATAN FIZIKAL

ID	KETERANGAN	PERANAN
7.1.1	**Perimeter Keselamatan Fizikal** Kawalan bertujuan untuk menghalang capaian tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan aset maklumat USIM. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: Perimeter keselamatan fizikal digunakan untuk melindungi aset, individu, dan persekitaran fizikal daripada ancaman, bahaya, atau kemungkinan kerosakan. Pelaksanaan kawalan ini melibatkan pelbagai strategi dan tindakan untuk memastikan keselamatan dalam ruang fizikal seperti bangunan, lokasi perindustrian, infrastruktur, atau kawasan penting lain. Berikut adalah beberapa unsur	Jabatan Keselamatan dan Penguatkuasaan, Jabatan Pembangunan dan Pengurusan Fasiliti

ID	KETERANGAN	PERANAN
	penting yang berkaitan dengan perimeter keselamatan fizikal: (a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (c) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (d) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia; (e) Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; (f) Memastikan kawasan-kawasan	

ID	KETERANGAN	PERANAN
	penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan (g) Memasang alat penggera atau kamera keselamatan.	

7.2 KEMASUKAN FIZIKAL

ID	KETERANGAN	PERANAN
7.2.1	**Kawalan Kemasukan Fizikal** Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis Universiti. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Setiap pegawai dan kakitangan USIM hendaklah mempamerkan kad pengenalan universiti sepanjang waktu bertugas. Semua kad pengenalan universiti hendaklah dikembalikan kepada USIM apabila pemegangnya telah bertukar, tamat perkhidmatan atau bersara; (b) Setiap pelawat hendaklah mendaftar dan mendapatkan pas pelawat di Kaunter Balai Kawalan Utama dan hendaklah dikembalikan selepas tamat lawatan; (c) Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan Aset ICT USIM; dan (d) Kehilangan kad pengenalan universiti hendaklah dilaporkan segera kepada Jabatan Keselamatan dan Penguatkuasaan.	Warga USIM, pembekal, pakar runding, pihak yang mempunyai urusan dengan perkhidmatan ICT USIM

ID	KETERANGAN	PERANAN
7.2.2	**Kawasan Penyerahan dan Pemunggahan** Pintu masuk seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan. USIM hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.	Warga USIM, pembekal, pakar runding, pihak yang mempunyai urusan dengan perkhidmatan ICT USIM

7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN

ID	KETERANGAN	PERANAN
7.3.1	**Keselamatan Pejabat, Bilik dan Kemudahan** Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi ialah seperti yang berikut:	BKP, Pentadbir Pusat Data, Warga USIM

ID	KETERANGAN	PERANAN
	(a) Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan bilik fail, bilik cetakan, bilik kawalan kamera litar tertutup (CCTV) dan pusat data perlu dihadkan daripada dicapai tanpa kebenaran; (b) Kawasan tempat bekerja, bilik dan tempat operasi ICT perlu dihadkan daripada dicapai oleh orang luar; dan (c) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan.	

7.4 PEMANTAUAN KESELAMATAN FIZIKAL

ID	KETERANGAN	PERANAN
7.4.1	**Pemantauan keselamatan fizikal** Premis fizikal harus dipantau oleh sistem pengawasan termasuk pengawal, penggera penceroboh, sistem pemantauan video seperti CCTV dan perisian pengurusan maklumat keselamatan fizikal sama ada diurus secara dalaman atau oleh penyedia perkhidmatan pemantauan.	Ketua PTJ, ICTSO, Jabatan Keselamatan dan Penguatkuasaan

ID	KETERANGAN	PERANAN
	Sistem pemantauan harus dilindungi daripada capaian yang tidak dibenarkan untuk mengelakkan maklumat pengawasan, seperti suapan video, daripada dicapai oleh orang yang tidak dibenarkan atau sistem diceroboh secara jarak jauh. Melaksanakan pemantauan secara berterusan di premis bagi mengelakkan capaian secara fizikal yang tidak dibenarkan. Capaian kepada bangunan yang menempatkan sistem kritikal harus dipantau secara berterusan untuk mengesan capaian yang tidak dibenarkan atau tingkah laku yang mencurigakan dengan: (a) Memasang sistem pemantauan video seperti CCTV untuk melihat dan merakam capaian ke kawasan sensitif di dalam dan di luar premis USIM; (b) Memasang, mengikut piawaian terpakai yang berkaitan, dan menguji pengesan sentuhan, bunyi atau gerakan secara berkala untuk	

ID	KETERANGAN	PERANAN
	mencetuskan penggera penceroboh seperti:	
	(i) Memasang pengesan sesentuh yang mencetuskan penggera apabila sesentuh dibuat atau pecah di mana-mana tempat di mana sentuhan boleh dibuat atau dipecahkan untuk digunakan sebagai penggera panik; (ii) Memasang pengesan yang sensitif kepada bunyi kaca pecah yang boleh digunakan untuk mencetuskan penggera bagi memberi amaran kepada kakitangan keselamatan; (c) Menggunakan penggera tersebut untuk melindungi semua pintu luar yang boleh dicapai. Kawasan yang tidak berpenghuni perlu sentiasa diberi perhatian; dan (d) Perlindungan juga perlu disediakan untuk kawasan lain (contoh komputer atau bilik komunikasi).	

7.5 PERLINDUNGAN DARIPADA ANCAMAN FIZIKAL DAN PERSEKITARAN

ID	KETERANGAN	PERANAN
7.5.1	**Perlindungan Daripada Ancaman Fizikal dan Persekitaran** Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. USIM perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	Pengarah SDEC, ICTSO, Ketua Jabatan Keselamatan dan Penguatkuasaan

7.6 BEKERJA DI KAWASAN SELAMAT

ID	KETERANGAN	PERANAN
7.6.1	**Bekerja di Kawasan Selamat** Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga USIM yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis USIM termasuklah Pusat Data.	Ketua PTJ ICTSO, Pengarah SDEC, Jabatan Keselamatan dan Penguatkuasaan

ID	KETERANGAN	PERANAN
	Kawasan larangan perlu dilindungi daripada ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan hendaklah dipantau oleh pihak berikut: (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 yang bersesuaian; (b) Akses adalah terhad kepada warga USIM yang telah diberi kuasa sahaja dan dipantau pada setiap masa; (c) Pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) kamera atau lain-lain peralatan yang sesuai; (d) Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual; (e) Penggunaan kad akses, biometrik (cap jari, wajah) untuk mengelakkan akses tanpa kebenaran; (f) Pemantauan suhu, kelembapan, asap dan kebocoran air dalam bilik	

ID	KETERANGAN	PERANAN
	server untuk mengelakkan kerosakan peralatan kritikal; (g) Pengawasan manual secara rondaan berkala oleh pegawai keselamatan mengikut jadual, terutama di luar waktu pejabat; (h) Semua aktiviti akses (masuk dan keluar) direkod secara log digital automatik dan diaudit secara berkala; (i) Amaran keselamatan dari peralatan fizikal (CCTV, dan alarm) disalurkan ke sistem pemantauan keselamatan pusat untuk tindak balas segera; (j) Setiap pengeluaran atau pemulangan kunci mesti direkod dalam buku log kawalan kunci bagi tempat larangan seperti Bilik Kebal, Pusat Data dan Bilik Cetak Kertas Peperiksaan dan kawasan seumpamanya; (k) Penggandaan kunci tanpa kebenaran adalah dilarang sama sekali. (l) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; (m) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang	

ID	KETERANGAN	PERANAN
	bertanggungjawab di sepanjang tempoh di lokasi berkaitan; (n) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; (o) Mengehadkan jalan keluar masuk ke bilik server; dan (p) Bahan-bahan yang mudah terbakar tidak boleh berada di dalam bilik server.	

7.7 POLISI MEJA KOSONG DAN SKRIN KOSONG

ID	KETERANGAN	PERANAN
7.7.1	**Polisi Meja Kosong dan Skrin Kosong** Polisi Meja Kosong dan Skrin Kosong bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna, pada paparan skrin komputer, mesin pencetak, mesin faksimile atau mesin pengimbas apabila pengguna tidak berada di tempatnya. Polisi Meja Kosong dan Skrin Kosong ialah satu set garis panduan yang digunakan	Warga USIM, pembekal, pakar runding, pihak yang mempunyai urusan dengan perkhidmatan ICT USIM

ID	KETERANGAN	PERANAN
	dalam pengurusan keselamatan maklumat dan keberkesanan dalam universiti untuk melindungi maklumat sensitif dan menjaga privasi pekerja. Objektif utama polisi ini adalah untuk memastikan data dan maklumat terjamin keselamatannya dan tidak didedahkan kepada pihak yang tidak mempunyai hak capaian ke atas data atau maklumat tersebut. Polisi ini merangkumi aspek-aspek berikut: (a) Penggunaan fungsi kata laluan penyelamat skrin (screen saver password) atau log keluar apabila meninggalkan komputer; (b) Penyimpanan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; (c) Semua dokumen hendaklah diambil segera daripada pencetak, pengimbas, mesin faksimile dan mesin fotostat; (d) Pengawalan e-mel masuk dan keluar; (e) Memastikan semua peranti mudah alih berada dalam keadaan terkawal bagi mengelakkan sebarang kecuaian; (f) Kawalan penggunaan mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas	

ID	KETERANGAN	PERANAN
	dan kamera digital (g) Penetapan dan hebahan peraturan serta panduan berkaitan konfigurasi mesej timbul (*pop-up message*) di skrin (contohnya mematikan *pop-up* e-mel dan mesej baharu semasa pembentangan, perkongsian skrin atau di kawasan awam); dan (h) Memadamkan maklumat sensitif atau kritikal pada papan putih dan jenis paparan lain apabila tidak diperlukan lagi.	

7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT

ID	KETERANGAN	PERANAN
7.8.1	**Penempatan dan Perlindungan Peralatan ICT** Peralatan 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 ialah seperti yang berikut: (a) Penggunaan kata laluan untuk	Warga USIM, pembekal, pakar runding, pihak yang mempunyai urusan dengan perkhidmatan ICT USIM

ID	KETERANGAN	PERANAN
	dicapai ke sistem komputer diwajibkan; (b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; (d) Pengguna dilarang membuat pemasangan sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem; (e) Pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; (f) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna; (g) Setiap pengguna adalah bertanggungjawab atas kerosakan	

ID	KETERANGAN	PERANAN
	atau kehilangan perkakasan ICT di bawah kawalannya; (h) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptible Power Supply* (UPS) dan Generator Set (Gen-Set); (i) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; (j) Peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci; (k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai; (l) Peralatan ICT yang hendak dibawa ke luar premis USIM, perlulah mendapat kelulusan Pegawai Aset PTJ dan direkodkan bagi tujuan pemantauan; (m) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden;	

ID	KETERANGAN	PERANAN
	(n) Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; (o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pegawai Aset; (p) Sebarang pertukaran penempatan dan pemilikan aset perlulah direkodkan di dalam sistem aset dan inventori universiti; (q) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pegawai Aset untuk dibaik pulih; (r) 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; (s) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal tanpa kebenaran Pentadbir Aset; (t) Pengguna dilarang sama sekali mengubah kata laluan ***password***	

ID	KETERANGAN	PERANAN
	administrator yang telah ditetapkan oleh pihak ICT; dan (u) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi kerajaan dan USIM sahaja.	

7.9 KESELAMATAN ASET DI LUAR PREMIS

ID	KETERANGAN	PERANAN
7.9.1	**Keselamatan Aset di Luar Premis** Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis Universiti. Peralatan yang dibawa keluar dari premis Universiti adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan (c) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.	Warga USIM, Pembekal Pihak yang mempunyai urusan berkaitan perkhidmatan ICT USIM

7.10 MEDIA STORAN

ID	KETERANGAN	PERANAN
7.10.1	**Pengurusan Media Boleh Alih (*Management of Removable Media*)** Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengelasan yang diguna pakai oleh USIM. Prosedur-prosedur pengendalian media yang perlu dipatuhi ialah seperti yang berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan (e) Menyimpan semua jenis media di tempat yang selamat.	Pegawai Aset Pentadbir Aset

ID	KETERANGAN	PERANAN
7.10.2	**Pelupusan Media** Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan; dan Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	Pegawai Aset, Pentadbir Aset

ID	KETERANGAN		PERANAN
7.10.3		**Pengalihan Aset** Perkakasan ICT yang hendak dibawa keluar dari premis USIM untuk tujuan rasmi, perlulah melalui langkah-langkah keselamatan seperti yang berikut: (a) Perlulah mendapat kelulusan Ketua Jabatan atau pegawai aset di PTJ yang dilantik dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan (b) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.	Pengguna, Pegawai Aset

ID	KETERANGAN	PERANAN
7.10.4	**Pengendalian Media** Melindungi aset maklumat daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	Warga USIM, Pengguna, Pegawai Aset

7.11 UTILITI SOKONGAN

ID	KETERANGAN	PERANAN
7.11.1	**Utiliti Sokongan** Memastikan utiliti premis dan semua peralatan sokongan ICT berada dalam keadaan baik untuk menjamin kesinambungan operasi dan mengurangkan risiko kegagalan perkhidmatan. (a) Semua utiliti sokongan (seperti bekalan elektrik, sistem penghawa dingin, UPS, dan generator) hendaklah diselenggara secara berkala sekurang-kurangnya setahun sekali atau mengikut keperluan pengeluar. (b) Penyelenggaraan perlu direkodkan, dipantau, dan disahkan oleh pihak bertanggungjawab. (c) Sebarang isu yang dikesan hendaklah dilaporkan dan ditangani segera untuk memastikan kelancaran operasi ICT.	JPPF, Warga USIM (staf)

7.12 KESELAMATAN KABEL

ID	KETERANGAN	PERANAN
7.12.1	**Keselamatan Kabel** Melindungi kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat daripada risiko pintasan, gangguan, atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil ialah seperti yang berikut: (a) Akses kepada laluan kabel hendaklah dikawal untuk mengelakkan gangguan atau pencerobohan; (b) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (c)	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	(c) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (d) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan pemintasan maklumat pada kabel; dan (e) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui sesalur kabel bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	

7.13 PENYELENGGARAAN PERALATAN

ID	KETERANGAN	PERANAN
7.13.1	**Penyelenggaraan Peralatan** Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: (a) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (b) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; (c) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;	Pegawai Aset, Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	(d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan (e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	

7.14 PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN

ID	KETERANGAN	PERANAN
7.14.1	**Pelupusan yang Selamat atau Penggunaan Semula Peralatan** 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 USIM dan ditempatkan di	Pegawai Aset, Pentadbir Sistem ICT, warga USIM

ID	KETERANGAN	PERANAN
	USIM. 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 USIM. Langkah-langkah seperti yang berikut hendaklah diambil: (a) Bagi peralatan ICT yang akan dilupuskan sebelum dipindah milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat; (b) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (c) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (d) Pelupusan aset maklumat hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;	

ID	KETERANGAN	PERANAN
	(e) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti yang berikut tanpa kebenaran USIM: (i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi; (ii) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hard disk*, *motherboard* dan sebagainya; (iii) Menyimpan dan memindahkan perkakasan luaran komputer seperti pembesar suara dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di agensi; (iv) Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; (v) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Universiti; Pengguna ICT bertanggungjawab memastikan segala maklumat rasmi kerajaan disalin pada media storan pendua	

ID	KETERANGAN	PERANAN
	sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan bagi tujuan sandaran maklumat; (a) 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; (b) Pegawai Aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori dan aset universiti.	

8 KAWALAN TEKNOLOGI

Terdapat 34 kawalan teknologi yang utama dan perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di USIM. Perincian kawalan teknologi seperti di bawah.

8.1 PERIMETER KESELAMATAN FIZIKAL (PHYSICAL SECURITY PARAMETER)

ID	KETERANGAN	PERANAN
8.1.1	**Polisi Peranti Mudah Alih** Polisi dan langkah-langkah keselamatan sokongan hendaklah digunakan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih. USIM perlu membangun serta menyebarkan dasar dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang dikenal pasti melalui penggunaan peranti titik akhir merangkumi perkara yang berikut: (a) jenis dan tahap klasifikasi maklumat yang digunakan oleh pengguna peranti titik akhir untuk mengendali, memproses, menyimpan atau menyokong kemudahan maklumat; (b) peraturan untuk capaian kepada perkhidmatan maklumat, rangkaian awam atau mana-mana rangkaian lain di luar premis; (c) perlindungan terhadap virus dan perisian hasad (*malware*); (d) Menyekat penggunaan keupayaan jarak jauh (*remote disabling*), pemadaman dan penguncian (lockout);	JKICT, JPICT, Pentadbir Sistem/Pengguna

ID	KETERANGAN	PERANAN
	(e) sandaran (*back up*); (f) penggunaan perkhidmatan web dan aplikasi web; (g) penggunaan perkhidmatan mudah alih (*portable service*), termasuk peranti memori mudah alih, dan kemungkinan untuk menghilangkan keupayaan port fizikal (contoh: *port USB, USB Type-C*); dan (h) penggunaan keupayaan pembahagian (*partitioning capabilities*) jika disokong oleh peranti titik akhir (*Endpoint Devices*) pengguna.	

8.2 HAK CAPAIAN ISTIMEWA

ID	KETERANGAN	PERANAN
8.2.1	**Pengurusan Hak Capaian Istimewa** Peruntukan dan penggunaan hak capaian istimewa hendaklah dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas merujuk kepada **Prosedur Pendaftaran dan Penamatan Pengguna.**	Pentadbir Sistem ICT

8.3 SEKATAN CAPAIAN MAKLUMAT

ID	KETERANGAN	PERANAN
8.3.1	**Sekatan Capaian Maklumat** Capaian kepada fungsi maklumat dan sistem ICT hendaklah dihadkan mengikut dasar kawalan capaian merangkumi perkara yang berikut: (a) tidak membenarkan pengguna yang tidak berdaftar mencapai maklumat terperingkat; (b) menyediakan mekanisme konfigurasi untuk mengawal capaian	Pengguna, Pentadbir Sistem, ICTSO, Pengarah SDEC

ID	KETERANGAN	PERANAN
	kepada maklumat dalam sistem, aplikasi dan perkhidmatan; (c) mengawal data yang boleh dicapai oleh pengguna tertentu; (d) mengawal identiti atau kumpulan identiti yang mempunyai hak capaian, seperti membaca, menulis, memadam dan melaksanakan (*execute*); (e) menyediakan kawalan capaian fizikal atau logikal untuk mengasingkan aplikasi sensitif, data aplikasi, atau sistem; dan (f) Pentadbir Sistem hendaklah melaksanakan semakan dan pemantauan secara berkala **sekurang-kurangnya setahun sekali** bagi memastikan pengguna yang mencapai sistem adalah sah. Penggunaan proses dan teknik pengurusan capaian yang dinamik (*dynamic access management*) bagi melindungi maklumat sensitif perlu dilaksanakan sekiranya diperlukan dengan mengambil kira keperluan berikut: (a) perlindungan sepanjang kitar hayat maklumat dengan menetapkan peraturan berdasarkan kes	

ID	KETERANGAN	PERANAN
	penggunaan; (b) mewujudkan operasi, proses memantau dan melapor serta infrastruktur sokongan teknikal; dan (c) melindungi data dengan menetapkan keperluan pengesahan, menghadkan capaian, melaksanakan penyulitan, menetapkan kebenaran mencetak, merekod capaian pengguna dan penggunaan maklumat serta memberikan amaran sekiranya terdapat percubaan untuk menyalahgunakan maklumat.	

8.4 KAWALAN CAPAIAN KEPADA KOD SUMBER

ID	KETERANGAN	PERANAN
8.4.1	**Kawalan Capaian Kepada Kod Sumber Program**	Pengurus Projek , Pentadbir Sistem ICT, Pengarah SDEC

ID	KETERANGAN	PERANAN
	Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan ialah seperti yang berikut: (a) Log audit perlu dikekalkan kepada semua capaian kepada kod sumber; (b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; (c) Kod sumber bagi semua sistem aplikasi atau kod sumber sistem aplikasi yang disesuaikan hendaklah menjadi hak milik USIM; (d) Mengurus capaian kepada kod sumber program dan perpustakaan sumber program (*program source libraries*) mengikut prosedur yang ditetapkan; dan (e) Memberi capaian baca dan tulis (*read and write*) kepada kod sumber berdasarkan keperluan dan berupaya mengawal risiko mengubah atau menyalah guna kod sumber berdasarkan prosedur yang ditetapkan.	

8.5 PENGESAHAN IDENTITI YANG SELAMAT

ID	KETERANGAN	PERANAN
8.5.1	**Prosedur Log Masuk yang Selamat** Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan ialah seperti yang berikut: (a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan USIM; (b) Menjana amaran (*alert*) sekiranya berlaku pelanggaran semasa proses log masuk terhadap aplikasi sistem; (c) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan yang kukuh dan berkualiti; dan (d) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem;	Pentadbir Sistem, ICTSO, Pengarah SDEC

8.6 PENGURUSAN KAPASITI

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

8.7 PERLINDUNGAN DARIPADA PERISIAN HASAD

ID	KETERANGAN	PERANAN
8.7.1	**Perlindungan daripada Perisian Hasad** Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada serangan perisian hasad hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Perkara yang perlu dilaksanakan bagi memastikan perlindungan aset maklumat daripada perisian hasad ialah seperti yang berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program perisian hasad seperti antivirus, *Intrusion Detection* System (IDS), *Intrusion Prevention System* (IPS) dan *Web Application Firewall* (WAF) serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang yang sedang	Pentadbir Sistem ICT, Pengguna

ID	KETERANGAN	PERANAN
	berkuat kuasa; (c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; (d) Mengemas kini antivirus dengan *signature*/*pattern* antivirus yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri program kesedaran mengenai ancaman perisian hasad dan cara mengendalikannya; (g) 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; (h) Menyediakan pelan kesinambungan perkhidmatan yang sesuai untuk pulih daripada serangan perisian hasad; (i) Menentukan prosedur dan tanggungjawab untuk menangani perlindungan terhadap perisian	

ID	KETERANGAN	PERANAN
	hasad pada sistem; dan (j) Mengesahkan ketepatan sumber maklumat yang berkaitan dengan perisian hasad. (k) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan.	

8.8 PENGURUSAN KERENTANAN TEKNIKAL

ID	KETERANGAN	PERANAN
8.8.1	**Pengurusan Kerentanan Teknikal (*Management of Technical Vulnerabilities*)** Maklumat berkaitan kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan universiti terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan terhadap keterdedahan teknikal perlu dilaksanakan untuk melindungi sistem maklumat, perisian, dan infrastruktur teknikal universiti daripada ancaman dan serangan yang berkaitan dengan kerentanan. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi; (b) Mengenal pasti, menilai dan menganalisis tahap risiko kerentanan yang wujud dalam sistem, perisian, dan rangkaian	Pentadbir Sistem ICT, CSIRT USIM

ID	KETERANGAN	PERANAN
	USIM; (c) Melaksanakan tindakan penambahbaikan untuk mengatasi kerentanan yang telah dikenal pasti, termasuk melaksanakan penambahbaikan keselamatan dan konfigurasi semula; (d) Memantau sistem dan perisian secara berterusan untuk mengenal pasti kerentanan yang mungkin muncul dalam masa sebenar; dan (e) Melaksana dan memastikan amalan terbaik dalam keselamatan teknikal dan pengurusan kerentanan.	

8.9 PENGURUSAN KONFIGURASI

ID	KETERANGAN	PERANAN
8.9.1	**Pengurusan konfigurasi** Pengurusan konfigurasi perlu dilaksanakan untuk memastikan perkakasan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul berserta dengan keperluan keselamatan. Konfigurasi tidak diubah tanpa kebenaran berdasarkan prosedur yang ditetapkan. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Melindungi capaian terhadap fail konfigurasi mengikut kawalan yang ditetapkan; (b) Merekod dan menyimpan sebarang perubahan konfigurasi dengan selamat; dan (c) Memantau konfigurasi untuk mengesahkan tetapan konfigurasi dan menilai kawalan keselamatan.	Pentadbir Sistem

8.10 PENGHAPUSAN MAKLUMAT

ID	KETERANGAN	PERANAN
8.10.1	**Penghapusan Maklumat** Maklumat terperingkat yang disimpan dalam aset maklumat hendaklah dilupuskan mengikut prosedur yang ditetapkan. Perkara yang perlu dipatuhi ialah seperti berikut: (a) Menentukan kaedah penghapusan maklumat yang sesuai selaras dengan keperluan USIM; (b) Merekod keputusan sebagai bukti penghapusan maklumat; dan (c) Mendapatkan bukti penghapusan maklumat jika menggunakan perkhidmatan pembekal.	Pemilik Maklumat Pemilik Aset Pegawai Aset

8.11 PENYEMBUNYIAN DATA

ID	KETERANGAN	PERANAN
8.11.1	**Penyembunyian data (*Data Masking*)** Penyembunyian data dilaksanakan bagi melindungi data sensitif seperti data *Personally Identifiable Information* (PII), dan data terperingkat dengan mengambil kira keperluan perkhidmatan dan polisi kawalan capaian serta polisi lain yang berkaitan tertakluk kepada keperluan perundangan dan peraturan yang berkuat kuasa. Pelaksanaan penyamaran data ialah berdasarkan prosedur yang ditetapkan. Penyembunyian data diperlukan bagi melindungi data PII dan data sensitif daripada terdedah atau bocor kepada pihak yang tidak bertanggungjawab yang akan menyebabkan imej USIM terjejas. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Mengenal pasti klasifikasi data yang perlu dikongsi dengan pihak ketiga; (b) Mengenal pasti teknik yang sesuai selaras dengan sensitiviti data; dan (c) Memastikan pengguna hanya dapat mencapai data yang minimum yang dibenarkan sahaja.	Pemilik Maklumat, Pentadbir Sistem

8.12 PENCEGAHAN KETIRISAN DATA

ID	KETERANGAN	PERANAN
8.12.1	**Pencegahan ketirisan Data (*Data Leakage*)** Data dalam sistem, rangkaian dan peralatan lain perlu dilindungi daripada pendedahan dan pengekstrakan data yang tidak sah oleh individu atau sistem. Perkara yang perlu dipatuhi ialah seperti berikut: (a) Mengenal pasti dan mengelaskan maklumat untuk dilindungi daripada ketirisan; (b) Memantau saluran transaksi dan perkongsian data (contohnya e-mel, pemindahan fail, perkhidmatan peranti atau media mudah alih); dan (c) Melaksanakan tindakan pengukuhan untuk mengelakkan ketirisan maklumat.	Pemilik Maklumat Pentadbir Sistem

8.13 SANDARAN MAKLUMAT

ID	KETERANGAN	PERANAN
8.13.1	**Sandaran Maklumat (*Backup of Information*)** Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara berkala mengikut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di *off site*. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi; (c) Menguji sistem sandaran sedia ada secara berkala **sekurang-kurangnya setahun sekali** bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	khususnya pada waktu bencana; dan (d) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara **harian, mingguan, bulanan atau tahunan**. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang-kurangnya **TIGA (3) GENERASI.**	

8.14 LEWAHAN BAGI KEMUDAHAN PEMPROSESAN MAKLUMAT

ID	KETERANGAN	PERANAN
8.14.1	**Lewahan bagi Kemudahan Pemprosesan Maklumat (*Redundancy of Information Processing Facilities*)** USIM perlu mengenal pasti keperluan, mereka bentuk dan melaksanakan lewahan untuk memastikan kesinambungan perkhidmatan dan ketersediaan kemudahan pemprosesan maklumat. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Mengenal pasti keperluan dan tahap kritikal bagi ketersediaan perkhidmatan dan sistem maklumat; (b) Menyediakan lewahan bagi kemudahan pemprosesan maklumat yang dikenal pasti;	Pentadbir Pusat Data, Pemilik, Pentadbir Sistem ICT.

ID	KETERANGAN	PERANAN
	(c) Menguji keberkesanan (*failover testing*) untuk memastikan keberkesanan kemudahan lewahan secara berkala; dan (d) Menyediakan mekanisme yang bersesuaian untuk memberi amaran gangguan atau kegagalan kemudahan pemprosesan maklumat kepada pemilik sistem untuk memastikan lewahan tersebut boleh mengambil alih fungsi kemudahan utama dibaiki atau diganti.	

8.15 PENGELOGAN MAKLUMAT

ID	KETERANGAN	PERANAN
8.15.1	**Menyediakan Log** 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 dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan.	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti yang berikut: (a) Fail log sistem pengoperasian; (b) Fail log perkhidmatan (*service*) (contoh: *web*, e-mel); (c) Fail log aplikasi (*audit trail*); dan (d) Fail log rangkaian (contoh: *switch, firewall, IPS*).	

ID	KETERANGAN	PERANAN
8.15.2	**Perlindungan Maklumat Log** Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada perubahan dan capaian tanpa izin merangkumi perkara berikut: (a) Pengguna, termasuk mereka yang mempunyai hak capaian istimewa, tidak diberi kebenaran untuk memadam atau menyahaktifkan log aktiviti mereka sendiri; dan (b) Kemudahan pengelogan	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	beroperasi dengan baik.	

ID	KETERANGAN	PERANAN
8.15.3	**Analisis Log** Analisis log perlu merangkumi analisis dan interpretasi aktiviti keselamatan maklumat untuk mengenal pasti aktiviti yang luar biasa atau tingkah laku yang janggal yang menunjukkan indikator sistem terjejas. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Memantau penggunaan kemudahan memproses maklumat secara berkala; (b) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak secara berkala dan laporan perlu disediakan jika perlu; (c) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;	Pentadbir Sistem ICT, CSIRT USIM

ID	KETERANGAN	PERANAN
	(a) Log Audit yang merekodkan semua aktiviti perlu diwujudkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan (b) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada pasukan CSIRT USIM.	

8.16 AKTIVITI PEMANTAUAN

ID	KETERANGAN	PERANAN
8.16.1	**Aktiviti Pemantauan** Rangkaian, sistem dan aplikasi harus dipantau dan tindakan sewajarnya diambil untuk menilai kemungkinan insiden keselamatan maklumat. Pentadbir Sistem perlu memantau untuk mengesan tingkah laku tidak normal (anomali) dan kemungkinan berlaku insiden keselamatan maklumat. Aktiviti pemantauan perlu merangkumi perkara seperti yang berikut: (a) Trafik keluar (*outbound*) dan masuk (*inbound*) bagi rangkaian, sistem dan aplikasi; (b) Capaian kepada sistem, pelayan, peralatan rangkaian, sistem pemantauan, aplikasi kritikal; (c) Log daripada peralatan keselamatan (contohnya antivirus, IDS, sistem pencegahan pencerobohan (IPS), penapis web, *firewall*, pencegahan kebocoran data);	Pentadbir Sistem, CSIRT USIM, IOC

ID	KETERANGAN	PERANAN
	(d) Log peristiwa yang berkaitan dengan sistem dan aktiviti rangkaian; (e) Memastikan supaya kod sumber yang dilaksanakan telah diberi kebenaran untuk dilaksanakan dan tidak diubah tanpa kebenaran; dan (f) Penggunaan dan prestasi sumber.	

8.17 PENYEGERAKAN JAM

ID	KETERANGAN	PERANAN
8.17.1	**Penyegerakan Jam** Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut waktu piawai Malaysia. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam USIM atau domain keselamatan perlu diseragamkan dengan waktu piawai Malaysia yang ditetapkan oleh National Metrology Institute of Malaysia (NMIM).	Pentadbir Pusat Data

8.18 PENGGUNAAN PROGRAM UTILITI YANG MEMPUNYAI HAK ISTIMEWA

ID	KETERANGAN	PERANAN
8.18.1	**Penggunaan Program Utiliti yang Mempunyai Hak Istimewa (*Use of Privileged Utility Programs*)** Penggunaan program utiliti yang boleh mengatasi (*overriding*) kawalan sistem dan aplikasi hendaklah dikawal dan dihadkan kepada pegawai yang dibenarkan sahaja. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Had penggunaan program utiliti kepada bilangan praktikal minimum pengguna yang dipercayai dan dibenarkan; (b) Penggunaan prosedur pengenalan, pengesahan dan kebenaran untuk program utiliti, termasuk pengenalan unik pengguna program utiliti; (c) Mentakrif dan mendokumentasikan tahap kebenaran untuk program utiliti; (d) Kebenaran untuk menggunakan program utiliti secara ad hoc; (e) Melaksanakan pengasingan tugas dengan menghadkan capaian pengguna yang mempunyai	Pengguna, Pengurus Projek, Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	capaian kepada program utiliti; (f) Mengalih keluar atau melumpuhkan semua program utiliti yang tidak diperlukan; (g) Menghadkan ketersediaan program utiliti; dan (h) Pengelogan semua penggunaan program utiliti.	

8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI

ID	KETERANGAN	PERANAN
8.19.1	**Pemasangan Perisian pada Sistem yang Beroperasi** Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus ialah seperti yang berikut: (a) Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian; (b) Aplikasi dan sistem operasi hanya	Pengarah SDEC, Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; (c) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur; (d) Pengemaskinian perisian operasi hanya boleh dilaksanakan oleh pentadbir terlatih atas kebenaran pengurusan; (e) Memastikan bahawa hanya kod boleh laksana (*executable code*) yang telah diluluskan dan tiada kod pembangunan atau pengkompil (*compilers*) dipasang pada sistem operasi; (f) Mengemas kini semua perpustakaan sumber (*source libraries*) program yang sepadan; (g) Menggunakan sistem kawalan konfigurasi untuk mengekalkan kawalan semua perisian operasi serta dokumentasi sistem; (h) Mengarkibkan versi lama perisian, bersama-sama dengan semua maklumat dan parameter, prosedur, butiran konfigurasi dan perisian sokongan yang diperlukan sebagai langkah luar jangka (*contingency*),	

ID	KETERANGAN	PERANAN
	dan selagi perisian itu diperlukan untuk membaca atau memproses data yang diarkibkan.	

8.20 KESELAMATAN RANGKAIAN

ID	KETERANGAN	PERANAN
8.20.1	**Kawalan Rangkaian** Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas daripada risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan	Ketua Bahagian, Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	dihadkan kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; (e) Tembok keselamatan (*firewall*) hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Sistem ICT; (f) Semua trafik keluar dan masuk rangkaian USIM hendaklah melalui firewall di bawah kawalan USIM. (g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna KECUALI mendapat kebenaran daripada Pegawai Keselamatan Teknologi Maklumat (ICTSO); (h) Memasang perisian IPS bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat Kerajaan; (i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; (j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan	

ID	KETERANGAN	PERANAN
	SDEC USIM tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di USIM sahaja dan penggunaan modem, router, switch dan lain-lain adalah dilarang sama sekali melainkan dengan kelulusan daripada ICTSO; (l) Kemudahan bagi rangkaian tanpa wayar (*wireless*) USIM hendaklah dipantau dan dikawal penggunaannya; (m) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan; (n) Menempatkan atau memasang antara muka (*interfaces*) yang bersesuaian antara rangkaian USIM, rangkaian agensi lain dan rangkaian awam; (o) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; (p) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian	

ID	KETERANGAN	PERANAN
	ICT yang dibenarkan sahaja; (q) Mengawal capaian fizikal dan logikal ke atas kemudahan *port* diagnostik dan konfigurasi jarak jauh; (r) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan USIM; dan (s) Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap peraturan USIM. Semua peralatan yang hendak disambung kepada rangkaian perlu bebas daripada virus dan mempunyai antivirus yang sah; (t) Capaian kepada rangkaian perlu dilaksanakan mengikut kategori yang telah ditetapkan iaitu Intranet, Internet dan *Demilitarized Zone* (DMZ); (u) Sistem yang terdapat dalam rangkaian Intranet tidak dibenarkan dicapai dari Internet; (v) Pihak ketiga tidak dibenarkan untuk mencapai rangkaian Intranet kecuali untuk kerja-kerja pembangunan atau penyelenggaraan sistem dengan kebenaran USIM; dan	

ID	KETERANGAN	PERANAN
	(w) Capaian kepada rangkaian tanpa wayar hendaklah dikawal mengikut kategori pengguna.	

8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN

ID	KETERANGAN	PERANAN
8.21.1	**Keselamatan Perkhidmatan Rangkaian** Pengurusan bagi semua perkhidmatan rangkaian dalaman dan sumber luar yang merangkumi mekanisme keselamatan dan tahap serta keperluan perkhidmatan rangkaian hendaklah dikenal pasti dan dimasukkan dalam perjanjian perkhidmatan.	ICTSO, Pengarah SDEC, Pentadbir Sistem ICT, Pembekal

8.22 PENGASINGAN RANGKAIAN

ID	KETERANGAN	PERANAN
8.22.1	**Pengasingan dalam Rangkaian** Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian di USIM.	ICTSO, Pengarah SDEC, Pentadbir Sistem ICT

8.23 PENAPISAN WEB

ID	KETERANGAN	PERANAN
8.23.1	**Penapisan Web (*Web Filtering*)** Kawalan penapisan web dalam bentuk perisian atau sebagainya perlu dilaksanakan bagi mengesan dan menyekat ke laman web yang dianggap tidak selamat dan tidak sesuai. Ini bagi melindungi sistem maklumat daripada sebarang ancaman keselamatan laman web luaran. USIM hendaklah mengurangkan risiko mencapai laman web yang mengandungi maklumat yang dilarang atau diketahui mengandungi virus atau data pancingan	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	(*phishing*) data oleh pengguna. USIM hendaklah mengenal pasti jenis laman web yang patut atau tidak boleh dicapai oleh warga USIM. USIM hendaklah mempertimbangkan untuk menyekat capaian kepada jenis laman web yang berikut: (a) Laman web yang mempunyai fungsi muat naik maklumat melainkan dibenarkan atas sebab perkhidmatan yang sah; (b) Tapak web yang diketahui atau disyaki berniat jahat; (c) Pelayan arahan dan kawalan (*command and control*); (d) Laman web berniat jahat yang diperoleh daripada risikan ancaman; dan (e) Laman web yang berkongsi kandungan haram.	

8.24 PENGGUNAAN KRIPTOGRAFI

ID	KETERANGAN	PERANAN
8.24.1	**Polisi Penggunaan Kawalan Kriptografi** Kriptografi merangkumi kaedah-kaedah seperti yang berikut: (a) **Penyulitan Data**: Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat penyulitan semasa dalam simpanan atau semasa sedang dipindahkan (data at rest / in transit); (b) **Tandatangan Digital**: Tandatangan digital digunakan bagi memastikan maklumat digital tulen dan mempunyai integriti serta tidak boleh disangkal.	Pemilik sistem Pentadbir sistem ICT

ID	KETERANGAN	PERANAN
8.24.2	**Pengurusan Infrastruktur Kunci Awam** Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah sijil digital tersebut.	ICTSO Pentadbir Sistem

8.25 KITAR HAYAT PEMBANGUNAN SISTEM YANG SELAMAT

ID	KETERANGAN	PERANAN
8.25.1	**Dasar Pembangunan Sistem yang Selamat** Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam sistem. Perkara yang perlu **dipertimbangkan** ialah seperti yang berikut: (a) Keselamatan persekitaran pembangunan; (b) Keselamatan pangkalan data; (c) Keperluan keselamatan dalam fasa reka bentuk; (d) Keperluan titik semak keselamatan dalam carta perbatuan projek; (e) Keperluan pengetahuan ke atas keselamatan aplikasi; (f) Keselamatan dalam kawalan versi; dan (g) (g) Bagi pembangunan menggunakan sumber, pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem	ICTSO, Pengarah SDEC, Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
8.25.2	**Kitar Hayat Pembangunan Sistem yang Selamat** Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. USIM perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: (a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; (b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; (c) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; (d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; (e) Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan (f) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	Pentadbir Sistem ICT, Pengarah SDEC

8.26 KEPERLUAN KESELAMATAN APLIKASI

ID	KETERANGAN	PERANAN
8.26.1	**Melindungi Perkhidmatan Aplikasi dalam Rangkaian Awam** Perkara yang perlu dipertimbangkan ialah seperti yang berikut: (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 USIM. Contoh perkhidmatan sumber luaran ialah: (i) Perisian Sebagai Satu Perkhidmatan; (ii) Platform Sebagai Satu Perkhidmatan; (iii) Infrastruktur Sebagai Satu Perkhidmatan; (iv) Storan Pengkomputeran Awan; dan (v) Pemantauan Keselamatan. (b) Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala;	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	(c) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan identiti (*authentication)*; (d) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; (e) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan (f) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	

ID	KETERANGAN	PERANAN
8.26.2	**Melindungi Transaksi Perkhidmatan Aplikasi** 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: (a) Penggunaan tandatangan digital oleh setiap pihak yang terlibat dalam transaksi; (b) Memastikan semua aspek transaksi dipatuhi: (i) Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan; (ii) Mengekalkan kerahsiaan maklumat; (iii) Mengekalkan privasi pihak yang terlibat; dan (iv) Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi; (c) Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh USIM.	ICTSO, Pengarah SDEC, Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
8.26.3	**Keperluan Keselamatan Aplikasi** Spesifikasi reka bentuk perlu mengandungi keperluan keselamatan sistem maklumat. Sekiranya sesuatu produk perisian aplikasi tersedia (*off-the-*shelf) diperoleh, pembekal perlu dimaklumkan berkenaan keperluan keselamatan.	Pentadbir Sistem ICT Pemilik Sistem

8.27 PRINSIP REKA BENTUK DAN KEJURUTERAAN SISTEM YANG SELAMAT

ID	KETERANGAN	PERANAN
8.27.1	**Prinsip Kejuruteraan Sistem yang Selamat** Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat.	Pentadbir Sistem ICT, Pengarah SDEC

8.27.2	**Prinsip Kejuruteraan Sistem Yang Selamat** Kawalan perubahan kepada perisian perlu dilaksanakan bagi mengurangkan risiko kerosakan pada perisian. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Proses pengemaskinian perisian atau sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang diberi tanggungjawab dan mengikut prosedur yang telah ditetapkan; (b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh digunakan selepas diuji dan diluluskan; (c) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; (d) Mengawal capaian ke atas kod atau cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (e) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal;	Pentadbir Sistem ICT Pembangun Sistem

ID	KETERANGAN	PERANAN
	dan (f) Semua sistem konfigurasi perlu didaftar dan didokumenkan.	

8.28 PENGATURCARAAN PROGRAM SELAMAT

ID	KETERANGAN	PERANAN
8.28.1	**Kawalan capaian kepada kod sumber** Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) Log audit perlu dikekalkan kepada semua akses kepada kod sumber; (b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; (c) Kod sumber bagi semua aplikasi dan perisian ialah hak milik USIM.	Ketua Projek, Pengurus Projek, Pentadbir Sistem ICT

8.29 PENGUJIAN DAN PENERIMAAN KESELAMATAN SISTEM

ID	KETERANGAN	PERANAN
8.29.1	**Pengujian Keselamatan Sistem** Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; (b) Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan. (c) Melakukan pengimbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem; (d) Menjalankan ujian penembusan untuk mengenal pasti kod dan reka bentuk yang tidak selamat; dan (e) Melaksanakan pengujian keselamatan sistem berdasarkan Garis Panduan Pasukan Projek Kluster Sistem Integrasi Aplikasi Universiti (SINAR)	Pentadbir Sistem ICT, ICTSO

ID	KETERANGAN	PERANAN
8.29.2	**Pengujian Penerimaan Sistem** 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: (a) Pengujian penerimaan sistem hendaklah merangkumi keperluan keselamatan sistem maklumat dan kepatuhan kepada polisi pembangunan selamat; (b) Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem diguna pakai; dan (c) Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian kerentanan (*vulnerability assessment*).	Pengguna, Pentadbir Sistem ICT, ICTSO

8.30 PEMBANGUNAN SISTEM OLEH SUMBER LUAR

ID	KETERANGAN	PERANAN
8.30.1	**Pembangunan oleh Sumber Luar** USIM hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan menggunakan sumber luar seperti pembekal. Kod sumber yang dibangunkan ialah **HAK MILIK USIM**. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Perjanjian lesen, kod sumber ialah **HAK MILIK USIM** dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi menggunakan sumber luar; (b) Bagi semua perkhidmatan yang disediakan oleh sumber luar, *Software as a Service* (SaaS) yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori "**Pembekal hendaklah membenar USIM hak mencapai kod sumber dan melaksanakan pengolahan risiko**"; (c) Keperluan kontrak untuk reka bentuk selamat, pengekodan dan	Pentadbir Sistem ICT, Pengarah SDEC, ICTSO

ID	KETERANGAN	PERANAN
	pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik; (d) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem; (e) Mengguna pakai prinsip dan tatacara *eskrow*; (f) Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian; (g) Penyediaan model ancaman (*threat modelling*) untuk dipertimbangkan oleh pembangun sistem serta memastikan tahap keselamatan minimum yang boleh diterima; dan (h) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data	

8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PRODUKSI

ID	KETERANGAN	PERANAN
8.31.1	**Pengasingan Persekitaran Pembangunan, Pengujian dan Produksi**	Pentadbir Sistem ICT, ICTSO

ID	KETERANGAN	PERANAN
	Persekitaran pembangunan, pengujian dan produksi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (*production*); (b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; (c) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat; (d) Menguji perubahan yang dilaksanakan dalam persekitaran ujian atau persekitaran sementara; (e) Tidak menguji dalam persekitaran produksi kecuali dalam keadaan yang telah ditentukan dan	

ID	KETERANGAN	PERANAN
	diluluskan; (f) Pengkompil, editor dan alat pembangunan atau program utiliti lain yang tidak boleh dicapai daripada sistem pengeluaran apabila tidak diperlukan; dan (g) Memaparkan label yang bersesuaian dengan persekitaran pada menu untuk mengurangkan risiko ralat.	

ID	KETERANGAN	PERANAN
8.31.2	**Persekitaran Pembangunan Selamat** Pemilik Sistem dan Pembangun Sistem hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. USIM perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: (a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; (b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; (c) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; (d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; (e) Pegawai yang bekerja dalam persekitaran pembangunan sistem berintegriti; dan (f) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	Pentadbir Sistem ICT, Pengarah SDEC

8.32 PENGURUSAN PERUBAHAN

ID	KETERANGAN	PERANAN
8.32.1	**Pengurusan Perubahan (*Change Management*)** Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara seperti yang berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;	Pentadbir Sistem ICT, Pengarah SDEC

ID	KETERANGAN	PERANAN
	(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; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.	

ID	KETERANGAN	PERANAN
8.32.2	**Prosedur Kawalan Perubahan Sistem** Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi ialah	Pengarah SDEC, Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	seperti yang berikut: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan Universiti. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal; (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; dan (d) Capaian kepada kod sumber aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.	

ID	KETERANGAN	PERANAN
8.32.3	**Kajian Semula Keperluan Teknikal bagi Aplikasi Selepas Perubahan Platform Pengoperasian** Apabila platform pengoperasian berubah, sistem penting hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan USIM. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Pengujian ke atas sistem hendaklah dilaksanakan untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform. (b) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan (c) Memastikan perubahan yang sesuai dibuat kepada Pelan Kesinambungan Perkhidmatan (PKP) USIM dan Pelan Pemulihan Bencana (DRP)	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
8.32.4	**Sekatan Ke atas Perubahan Dalam Pakej Perisian** Pengubahsuaian ke atas pakej perisian tidak digalakkan dan terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.	Pentadbir Sistem ICT, Pengarah SDEC

8.33 DATA PENGUJIAN

ID	KETERANGAN	PERANAN
8.33.1	**Perlindungan Data Ujian** Untuk memastikan perlindungan ke atas maklumat yang digunakan untuk pengujian. Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; (b) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian; (c) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai;	Pengguna, Pentadbir Sistem ICT, ICTSO

ID	KETERANGAN	PERANAN
	(d) Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar; (e) Melindungi maklumat sensitif melalui penyingkiran atau pengaburan data jika digunakan untuk ujian; Memadam maklumat operasi daripada persekitaran ujian serta-merta dengan betul selepas ujian selesai untuk mengelakkan penggunaan maklumat ujian tanpa kebenaran.	

8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PELAKSANAAN AUDIT

ID	KETERANGAN	PERANAN
8.34.1	**Kawalan Audit Sistem Maklumat** Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas fungsi penyampaian perkhidmatan USIM. Perkara berikut harus dipatuhi: (a) Bersetuju dengan permintaan audit untuk mencapai kepada sistem dan data dengan pengurusan yang sesuai; (b) Bersetuju dan mengawal skop ujian audit teknikal; (c) Mengehadkan ujian audit kepada capaian baca sahaja kepada perisian dan data. Jika capaian baca sahaja tidak tersedia untuk mendapatkan maklumat yang diperlukan, melaksanakan ujian oleh pentadbir berpengalaman yang mempunyai hak capaian yang diperlukan bagi pihak juruaudit; (d) Jika capaian diberikan, mewujudkan dan mengesahkan keperluan	ICTSO, Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	keselamatan peranti yang digunakan untuk mencapai sistem sebelum membenarkan capaian; (e) Hanya membenarkan capaian selain daripada baca sahaja untuk salinan terpencil fail sistem, memadamkannya apabila audit selesai, atau memberi mereka perlindungan yang sewajarnya jika terdapat kewajipan untuk menyimpan fail tersebut di bawah keperluan dokumentasi audit; (f) Mengenal pasti dan bersetuju dengan permintaan untuk pemprosesan khas atau tambahan, seperti menjalankan alat audit; (g) Menjalankan ujian audit yang boleh menjejaskan ketersediaan sistem di luar waktu perniagaan; (h) Memantau dan mengelog semua capaian untuk tujuan audit dan ujian.	

LAMPIRAN A

SURAT AKUAN PEMATUHAN

POLISI KESELAMATAN SIBER USIM

Nama (Huruf Besar) : …….....

No. Kad Pengenalan : …….....

Jawatan : …….....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber USIM; dan

Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : .....

Tarikh : .....

LAMPIRAN B

UNDANG-UNDANG, PEKELILING DAN DASAR YANG TERPAKAI

1. Akta Hak Cipta (Pindaan) Tahun 1997;
2. Akta Jenayah Komputer 1997;
3. Akta Komunikasi dan Multimedia 1998;
4. Akta Rahsia Rasmi 1972;
5. Akta Tandatangan Digital 1997;
6. Akta Keselamatan Siber 2024.
7. Arahan Teknologi Maklumat 2007;
8. Arahan Keselamatan;
9. Arahan Perbendaharaan;
10. Pekeliling Am Bilangan 3 Tahun 2000 Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
11. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi- Agensi Kerajaan;
12. Pekeliling Perbendaharaan 5 Tahun 2007 Tatacara Pengurusan Aset Alih Kerajaan (TPA);
13. Pekeliling Perkhidmatan Bil 5 2007 bertajuk Panduan Pengurusan Pejabat bertarikh 30 April 2007;
14. Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bilangan 3 Tahun 2015 Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastruktur (GPKI)];
15. Pekeliling Transformasi Pentadbiran Awam Bil.3 Tahun 2017 Pengurusan Komunikasi Bersepadu Kerajaan (Government Unified Communication (1GovUC));

16. Pekeliling Kemajuan Pentadbiran Awam Bil.1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam;
17. Pekeliling Am Bilangan 4 Tahun 2022 Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022;
18. Surat Pekeliling Am Bilangan 3 Tahun 2024 Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024;
19. Surat Pekeliling Am Bilangan 4 Tahun 2024 Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024;
20. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan;
21. Surat Arahan Ketua Pengarah MAMPU bertarikh 23 November 2007 Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-Agensi Kerajaan;
22. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS);
23. Perintah-Perintah Am;
24. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA);
25. PK 2.6: Perolehan Perkhidmatan Pengkomputeran Awan (Cloud) Sektor Awam;
26. Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan dalam Perkhidmatan Awam.
27. Pelupusan dokumen: Arahan Keselamatan dan tatacara Jabatan Arkib Negara.